

# Banker Omnia Vincit

**A tale of signed Brazilian bankers**

Malware Analysts Workforce

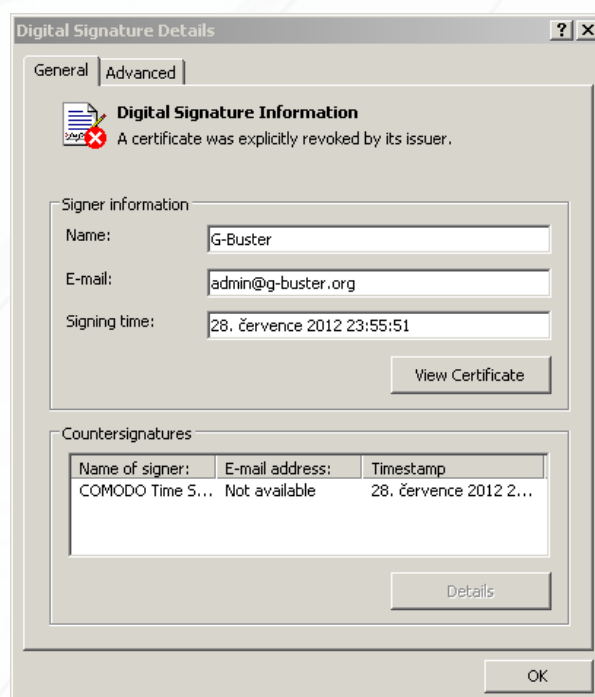
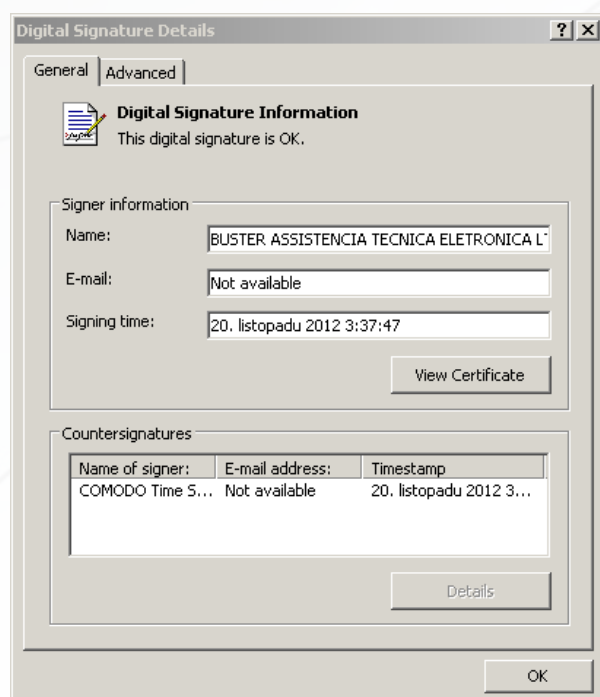
A few months ago we discovered an interesting South American malware for stealing banking data. We are very surprised that the “banker” used its own valid digital certificates.

The first assumption was that these certificates were stolen or modified, but it soon became clear that the certificates are original and have been created by COMODO and DigiCert Inc.

The attackers probably set up new companies that register digital certificates. All contact details are fictitious. The first certificates were registered with the COMODO. The last two certificates are registered with the DigiCert Inc. We assume that DigiCert has lower requirements for verification of customers in Brazil. Why painfully steal or edit certificates when you can buy your own?

These malicious certificates are using very similar or mangled names of legit bank security software manufacturers. One of the biggest companies developing anti-fraud solutions for Latin America’s online banking is GAS Tecnologia, and this malware focuses on their security solutions – such as browser plugins, virtual keyboards, two-factor authentication, and other useful techniques developed to secure online banking.

At the time of writing this, we have discovered the following digital certificates connected with this threat (some of them are already revoked):



## Certificate details:

CN	Gas Tecnology
O	Gas Tecnology
Street	R MOACIR AVIDOS 112 ap303
Street	Praia do Canto
L	Vitoria
S	Espirito Santo
Postal Code	29057-230
C	BR
Serial number	00 e4 d7 0e fc fd ca 6a fd 44 f9 70 07 bd 12 69 61
CN	COMODO Code Signing CA 2
O	COMODO CA Limited
L	Salford
C	Greater Manchester
S	GB
Sample SHA256	01E3D4D1782C4D84D3BAA6F7B9D719DE13A28A8DEF1EAE066E906C31A094F034

CN	G-Buster
O	G-Buster
Street	AV PAPA JOAO PAULO I 501
Street	APT 33 BLOCO D
L	SAO JOSE DOS CAMPOS
S	SP
Postal Code	12231-710
C	BR
Serial number	24 58 80 92 f6 62 31 ba 26 4c 14 e9 1a 69 3e b6
CN	COMODO Code Signing CA 2
O	COMODO CA Limited COMODO CA Limite
L	Salford
C	Greater Manchester
S	GB
Sample SHA256	BE9A396D3FA1B18C8D027DE0F221469A896AC5B727FE03307FE4F8317BC2240F

<b>CN</b>	G&P Projetos E Sistemas Ltda
<b>O</b>	G&P Projetos E Sistemas Ltda
<b>Street</b>	R MQ DE ITU 70
<b>Street</b>	VILA BUARQUE
<b>L</b>	SAO PAULO
<b>S</b>	SP
<b>Postal Code</b>	01223-903
<b>C</b>	BR
<b>Serial number</b>	3e 47 ed 11 80 a3 ba f6 be 2b eb 43 75 59 23 5d
<b>CN</b>	COMODO Code Signing CA 2
<b>O</b>	COMODO CA Limited
<b>L</b>	Salford
<b>C</b>	Greater Manchester
<b>S</b>	GB
<b>Sample SHA256</b>	6BB6E3E9C8F04E4F3E46A16C4D399940196A6A25B093F60CC95F6C32C5A08C51

<b>CN</b>	Buster Assistencia Tecnica Eeletronica Ltda - ME
<b>O</b>	Buster Assistencia Tecnica Eeletronica Ltda - ME
<b>L</b>	Sao Paulo
<b>S</b>	Sao Paulo
<b>C</b>	BR
<b>Serial number</b>	0a 38 9b 95 ee 73 6d d1 3b c0 ed 74 3f d7 4d 2f
<b>CN</b>	DigiCert Assured ID Code Signing CA-1
<b>OU</b>	www.digicert.com
<b>O</b>	DigiCert Inc
<b>C</b>	US
<b>Sample SHA256</b>	19557F26D50414C318055668B5E41F6C61CD0248E377C20920C86A4DAAD2C3FD

<b>CN</b>	Buster Paper Comercial Ltda
<b>O</b>	Buster Paper Comercial Ltda
<b>L</b>	Sao Jose Dos Campos
<b>S</b>	Sao Paulo
<b>C</b>	BR
<b>Serial number</b>	07 b4 4c db ff fb 78 de 05 f4 26 16 72 a6 73 12
<b>CN</b>	DigiCert Assured ID Code Signing CA-1
<b>OU</b>	www.digicert.com
<b>O</b>	DigiCert Inc
<b>C</b>	US
<b>Sample SHA256</b>	D57BCAD6497D06722734BC972A53F2E111CB9698079F70A1BE6D977711D7894C

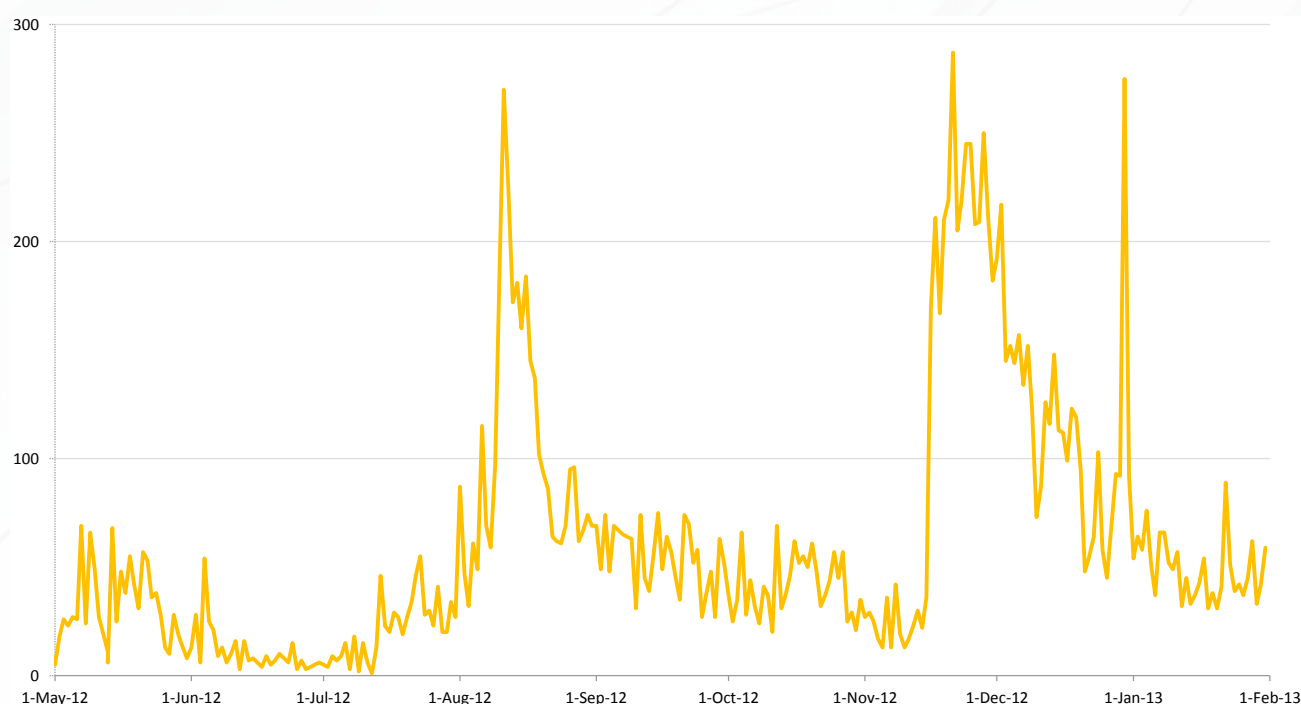
After searching our archives we were very surprised. The very first version of this family comes from the beginning of 2010, but without the signature. According to specific patterns, we have discovered dozens of builds and subsequent versions. The authors have come a long way during almost three years of evolution.

The first versions contained only one module targeting just a few banks (e.g. Banco Real, Caixa, HSBC). The malware was downloaded only from one URL (registered by malware authors!) and had almost no protections against reverse engineering.

Over time, the authors have added 2 additional modules, improved browser hijacking via DDE interface, and expanded the list of banks and other payment systems such as PayPal, VISA, etc. Download servers moved to large portals offering file-sharing services (e.g. Fileden, 4share, FileFactory, etc.)

In the latest evolution, the authors have added 5 valid digital certificates, changed downloads to support HTTPS/SSL, and also added other security features like encryption and anti-debug tricks. The changes are also in the number of targeted vendors – malware authors can steal credentials from 23 financial institutions and 5 e-commerce systems.

## Graph of banker detections per day:



## List of affected banks and payment systems:

American Express	Banrisul, Bradesco	MasterCard
Banco Bradesco	BrasilBank	PayPal
Banco do Brasil	BReal	REDECARD
Banco do Nordeste	CAIXA	Serasa Experian
Banco Itau	CELLCARD	Sicredi
Banco Rural	Cetelem	Visa
Banco Safra	CitiBank	
Banco Santander	HSBC Bank Brasil	



## List of affected e-commerce systems:

Cielo E-commerce  
CyberOffice eCommerce Manager  
EzCommerce  
VP-ASP Shopping Cart  
Zen Cart!

## Generic strings affecting other login pages:

Admin Login  
Administration  
Shop Manager  
Shopping Cart Control Panel  
Smart Card



Original webpage (HTML page):



**CAIXA**

## INTERNET BANKING CAIXA

**Já possuo usuário**

Usuário:

Acessar como: ☐ Pessoa Física  
☐ Pessoa Jurídica  
☐ Governo

Ir para:  **CONFIRMAR**

**Este é meu primeiro acesso no Internet Banking CAIXA**

Cadastre-se rapidamente em 3 passos

**INICIAR 1º PASSO**

**CUIDADO**  
com e-mails falsos



**CADASTRE-SE**

- > Conheça
- > Deficientes Visuais
- > Segurança
- > Esqueci a senha ou usuário

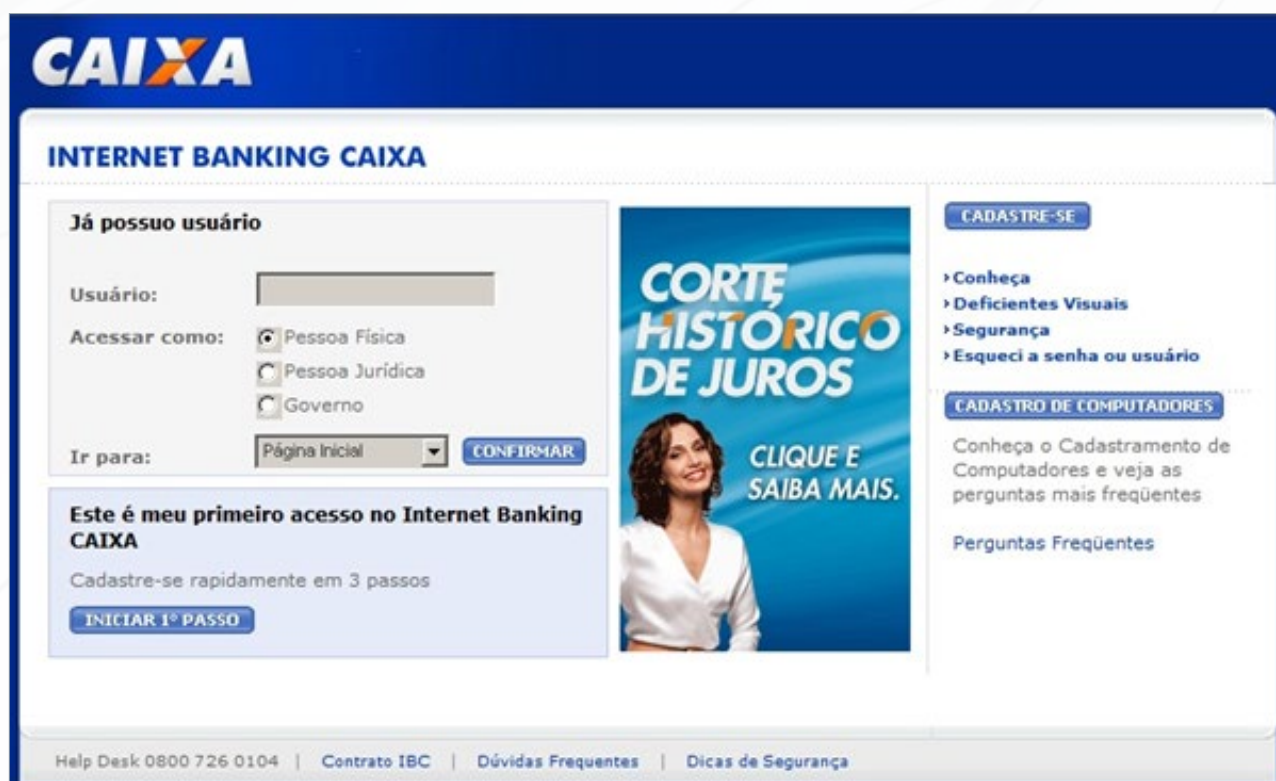
**CADASTRO DE COMPUTADORES**

Conheça o Cadastramento de Computadores e veja as perguntas mais frequentes

Perguntas Frequentes

Help Desk 0800 726 0104 | Contrato IBC | Dúvidas Frequentes | Dicas de Segurança

Hijacked webpage (Delphi GUI):



**CAIXA**

## INTERNET BANKING CAIXA

**Já possuo usuário**

Usuário:

Acessar como: ☒ Pessoa Física  
☐ Pessoa Jurídica  
☐ Governo


Ir para:  **CONFIRMAR**

**Este é meu primeiro acesso no Internet Banking CAIXA**

Cadastre-se rapidamente em 3 passos

**INICIAR 1º PASSO**

**CORTE HISTÓRICO DE JUROS**



**CLIQUE E SAIBA MAIS.**

**CADASTRE-SE**

- > Conheça
- > Deficientes Visuais
- > Segurança
- > Esqueci a senha ou usuário

**CADASTRO DE COMPUTADORES**

Conheça o Cadastramento de Computadores e veja as perguntas mais frequentes

Perguntas Frequentes

Help Desk 0800 726 0104 | Contrato IBC | Dúvidas Frequentes | Dicas de Segurança

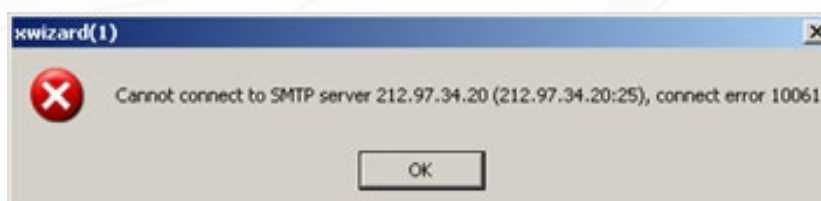
## A closer look at the latest version of the malware

The whole malware is written in Delphi and all functions such as communication, encryption, or browser hijacking are realized by use of third-party components (e.g. Indy Library, ZipForge, Delphi Encryption Compendium, etc.). This shows that the malware authors are not very technically gifted and prefer ready-made solutions instead of doing their own programming.

The malware does not attempt to spread in any way and also does not contain any form of remote control. We also cannot find spam-sending mechanisms or any other worm-spreading techniques such as USB infection. The malware also does not contain any driver, nor does it run any service – it's simple user land process.

All malware settings, URL addresses, and attackers' emails are hardcoded and authors cannot change anything on the fly. It is a very restrictive property. For example, if attackers want to change their email address, they must build a new version and re-infect all users.

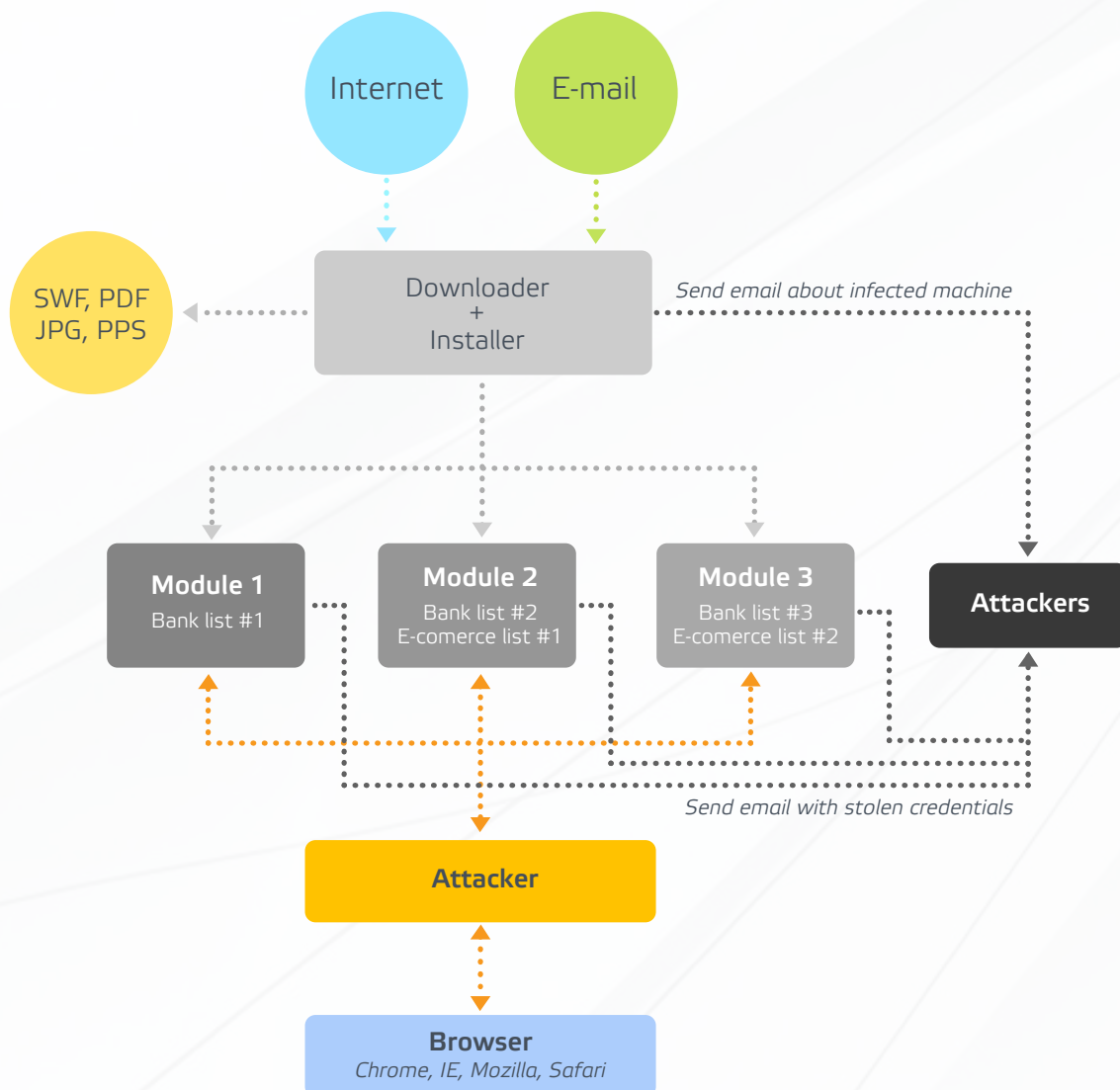
We also found a lot of implementation errors, most of them contained in a browser hijack via DDE interface, which operates only during the first connection to the client browser. Showing error message when connecting to SMTP server fails is also "uncommon."





The banking malware is split into two main parts, the **downloader** and the **main modules**.

### Modus operandi of the malware:



## Downloader

The downloader is most often spread through email or direct links from the Internet. It is a very simple and uninteresting application, and its authors added very poor anti-debug tricks and encryption.

Its main task is to “draw user attention” – the malware runs Flash animation, PDF, PowerPoint presentation, or just shows a simple image while downloading and installing all three modules. The downloader is digitally signed with a different certificate than the modules.

All URLs are encrypted and hardcoded as binary malware. Over the time the authors have tried many kinds of hosting for modules. The first modules were placed on personal web pages, and later authors moved them to large portals like FileFactory, 4share, etc. The latest downloader versions are also using HTTPS/SSL connections.

DNS	Standard query A som.egnys.com
DNS	Standard query response A 208.83.110.12
TCP	remote-as > https [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP	https > remote-as [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
TCP	remote-as > https [ACK] Seq=1 Ack=1 win=64240 Len=0
TLSv1	Client Hello
TCP	https > remote-as [ACK] Seq=1 Ack=71 win=65535 Len=0
TLSv1	Server Hello
TCP	[TCP segment of a reassembled PDU]
TCP	remote-as > https [ACK] Seq=71 Ack=2841 win=64240 Len=0
TCP	[TCP segment of a reassembled PDU]
TCP	remote-as > https [ACK] Seq=71 Ack=4261 win=62820 Len=0
TLSv1	Certificate, Server Hello Done

The downloader is disguised as Java (TM) Platform SE binary, whereas the modules have the names Live Update Wizard and Microsoft Corporation.

81DEA66CA020A6AE40...	4004	0.97 Java(TM) Platform SE binary	
WIDEAWAKE1.exe	2016	Live Update Wizard	
wwizard(1).exe	244	23.30 Microsoft Corporation	Microsoft Corporation
WIDEAWAKE2.exe	1988	LUUpdate	
wwizard(2).exe	2064	26.21 Microsoft Corporation	Microsoft Corporation
WIDEAWAKE3.exe	2080	LUUpdate	
wwizard(3).exe	2092	40.78 Microsoft Corporation	Microsoft Corporation

Downloader behavior:

```
[dropped files]
* C:\WINDOWS\win_pwr.pdf
// Module 1
* C:\WINDOWS\WIDEAWAKE1.zip
* C:\WINDOWS\WIDEAWAKE1.ec1
* C:\WINDOWS\WIDEAWAKE1.src
* C:\WINDOWS\xwizard(1).exe
* C:\WINDOWS\yw22.zip
* C:\WINDOWS\A777(1).txt
* C:\WINDOWS\A777(1)(2).txt
* C:\WINDOWS\system32\GpPlugin-Módulo de Segurança.exe

[changes to registry]
// Module 1
* sets value: "C:\WINDOWS\WIDEAWAKE1.exe"="Live update wizard" in key "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache"
* sets value: "Default"="1bdb9605b8d65c32db792cddb311329ef88ba419f8672d03c" in key "HKLM\Software\Classes\In2082592921v.gpn"
* sets value: "Calculator"="C:\WINDOWS\xwizard(1).exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
* sets value: "Calculator2"="C:\WINDOWS\xwizard(1).exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
// Module 2
* sets value: "C:\WINDOWS\WIDEAWAKE2.exe"="LUupdate" in key "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache"
* sets value: "C:\WINDOWS\xwizard(2).exe"="Microsoft Corporation" in key "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache"
* sets value: "Default"="7177a85e8ee365b6cd2ab11549eec800ff9aa4b164c9ea66" in key "HKLM\Software\Classes\ex1835213942d.1st"
* sets value: "WinEX7"="C:\WINDOWS\xwizard(2).exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
* sets value: "WinEX72"="C:\WINDOWS\xwizard(2).exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
// Module 3
* sets value: "C:\WINDOWS\WIDEAWAKE3.exe"="LUupdate" in key "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache"
* sets value: "Default"="9443ebdf2444fee810b9a5ffa45a070f47bf42ca1f8053e6" in key "HKLM\Software\Classes\bk2122467995s.1jj"
* sets value: "Notepad"="C:\WINDOWS\xwizard(3).exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
* sets value: "Notepad2"="C:\WINDOWS\xwizard(3).exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
```

## Main modules

Each module includes a valid digital signature, faked forms with customized graphics, and a list of banks, payment systems, and e-commerce systems for a browser hijack.

New modules were built during its evolution, probably because of the excessive file size – the decrypted and unpacked binaries were 17MB, 35MB, and 57MB! When the first module was too long, the authors simply added a new module containing code for other banks.

The third module was created around the end of 2010. Since then, the authors just adapted their content to match changes in the affected websites.

The modules also contain a mechanism for sending stolen credentials via email, and the malware uses large servers such as `smtp.mail.yahoo.com`, `smtp.mail.it`, etc.

```
C:\WINDOWS\WLog777.txt & C:\WINDOWS\WLog777.txt & C:\WINDOWS\WLog777.txt  
operatingnewlife@yahoo.com da7~0d4~0 !! + @ → operatingnewlife@yahoo.com  
operatingnewlife@yahoo.com i4~0D4~0 !! @ / @ L umanodourado2010.2@gmail.com  
ail.com 5~0 5~0, umanodourado2010.2@gmail.com. ‡ d9~0@ o ‡  
5~0 5~0| umanodourado2010.2@gmail.com ic15~0i5~0á umanodourado2010.2@gmail.com  
od$5~0$5~0! gmail.co‡ ‡ ‡ gmail. n5~0n5~0< umanodourado2010.2@gmail.c  
!! ‡ com -6~0-6~0 ‡ / @ L umanodourado2010.2@gmail.com D4~0s6~0  
‡ !! @ # @ Saborosas Manhãs 2012 X6~0t7~0 2 E6~0E6~0 @ Saborosas Manhãs 2012  
> @ Eu Te Adoro 2012 / Saborosas Manhãs 2012 s6~0X7~0 m <7~0<7~0 # ‡ !! smtp.mail.yahoo.com t7~0a7~0 ‡ !!  
+ @ → operatingnewlife@yahoo.com x7~0i4~0 ‡ !! qweqwe99 - ‡ A -7~0@ - ‡ A r>@
```

## Installation

After the download is complete, the malware sequentially triggers each module. When a module runs, it renames itself to the name of an official plugin and next checks if the other modules run in the memory, otherwise they are executed via ShellExecuteA API call.

We found another bug during the analysis: The malware creators forgot to update new modules and they try to execute them using the filenames from the previous versions.

The banker malware also sends an email with the data of the infected machine (e.g. MAC address, HD serial, Username, Machine name), and then the malware attempts to hijack the Internet browser.

```

02D02A24 $*a ASCII "Qweqwe99"
02CF2EC0 L,a ASCII "words_are_very_unnecessary@yahoo.com"
02CF2D00 a-a ASCII "smtp.mail.yahoo.com"
02D02A00 ?*a ASCII " "
02CF2DF8 o-a ASCII "Me Traz Um Sapo Doido"
02D02A90 E*a ASCII "enjoy.the.silence@hackermail.com"
02D02A50 \*a ASCII "words_are_very_unnecessary@yahoo.com"
02D02A30 <*a ASCII "Enjoy the Silence"
02D00A28 (a ASCII " "
02D019F4 ~+a ASCII " "
02D009F4 ~a ASCII " "
02CF2D68 h-a ASCII "00000000"
02CFE788 k-a ASCII "Serial HD:00000000"
02CFE7A8 E-a ASCII "00-00-00-00-00-00"
02CF3E0C ?>a ASCII "Mac Address:00-00-00-00-00-00"
02CF2DA8 E-a ASCII " "
02CF2D88 t-a ASCII "Um Ano Dourado 2010"
02D01C20 L-a ASCII "\Gb.zip"
02CF2D10 >-a ASCII "C:\Documents and Settings\ \My Documents\Gb.zip"
02CF2CEC g,a ASCII "C:\WINDOWS\WLogE2.txt"
02CF2CC8 E,a ASCII "C:\WINDOWS\WLogE2.txt"

```

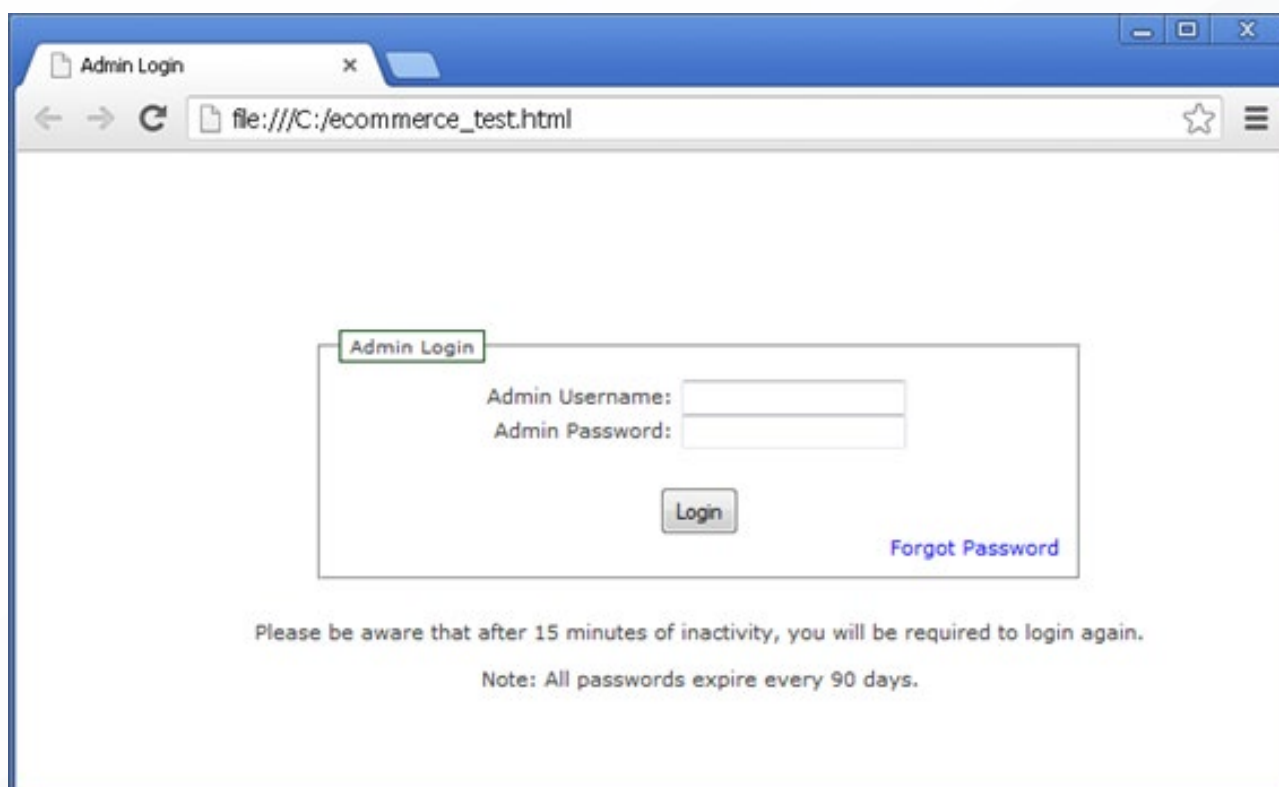
## Browser hijack

All data from the pages of banking institutions and online banking systems are stolen via a method called browser hijacking.

All spoofed entry or login forms, virtual keyboards, and other security elements are implemented using the Delphi GUI, so the malware has full access to all filled data. The authors created a lot of imitations, including the surrounding web graphics and other design parts. Some fake sites are very precise, whereas some are outdated and do not correspond well to the state of the original site.

In some cases, the authors use screenshots of the entire site, complete with some form elements. This site is very suspicious because there is nothing to mark or anything to click except the login forms and buttons.

The browser hijack method is using a very old DDE\* interface, but it is quite effective and almost browser-version independent. The following image shows injected data to a blank page in Chrome browser (v23.0.1271.95m).



## \* What is DDE?

Dynamic Data Exchange is a method of interprocess communication so that one program can communicate with or control another program. The primary function of DDE is to allow Windows applications to share data. For example, a cell in Microsoft Excel could be linked to a value in another application and, when the value changes, it would be automatically updated in the Excel spreadsheet. The same method we can use for a browser. Nowadays, DDE has been replaced by newer technologies such as OLE Automation, .NET Remoting, etc.

Access to the browser via DDE realized in Delphi code looks like this:

```
ClientDDE:= TDDEClientConv.Create(nil);  
with ClientDDE do  
begin  
    SetLink('IExplore','WWW_GetWindowInfo');  
    temp := (RequestData('0xFFFFFFFF'));  
    TempURL := StrPas(temp);  
    StrDispose(temp);  
    if MatchTarget(TempURL) = true then  
    begin  
        SetLink('IExplore','WWW_OpenURL');  
        RequestData(RedirectURL);  
    end;  
    CloseLink;  
    ClientDDE.Free;  
end;  
end;
```

DDE monitor logfile:

```
Task: String Created ["GbPlugin-Módulo de Segurança"]  
Task: Conversation established : Service="iexplore" Topic="WWW_GetWindowInfo"  
Task: String Created ["0xFFFFFFFF"]  
Task: String Created ["iexplore"]  
Task: String Created ["WWW_GetWindowInfo"]  
Task: Message [DDE_DATA] Format="TEXT" Value="http://caixa.gov.br/"
```



## Injecting code and stealing credentials

After a successful browser hijack, the malware checks the page loaded in the browser and waits until the user enters one of the affected bank websites.

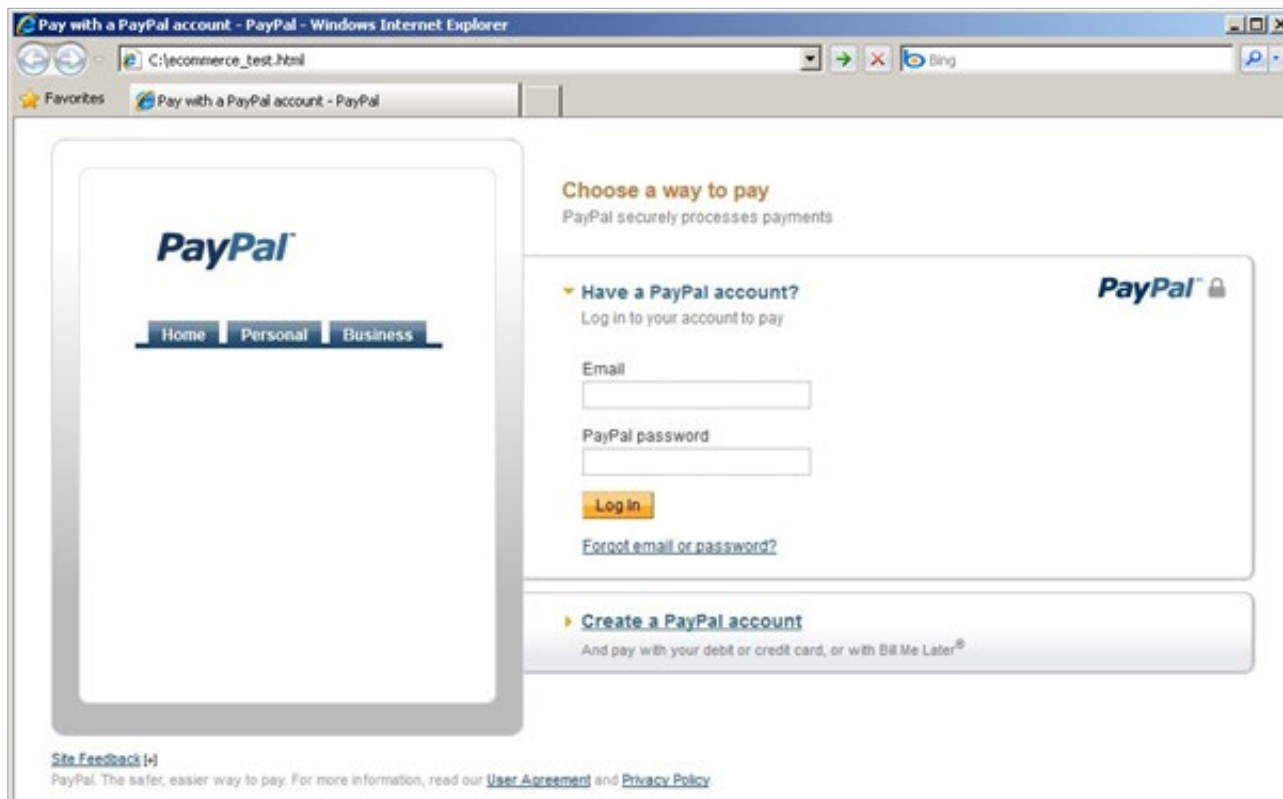
The malware is guarding the browser address bar and windows caption where the content of HTML <TITLE> tag is displayed. Once the malware encounters the appropriate address there, it starts to inject its own pieces of code and graphics. The attackers are replacing most often the login forms, virtual keyboards, error messages, and other security features.

The attacks on the banking sector are quite frequent nowadays and there is a lot of malware that does this stuff in far more sophisticated way (e.g. Zeus, Citadel, etc.).

Another interesting aspect of this banker malware includes attacks on the e-commerce sphere. Attackers focus of the login information to the administration environment, to get access to the entire e-commerce system, as well as payment or personal information on thousands of users.

The attackers can also steal data from payment systems such as PayPal (including Brazilian localization) or from the CellCard website (pre-paid SIM cards).

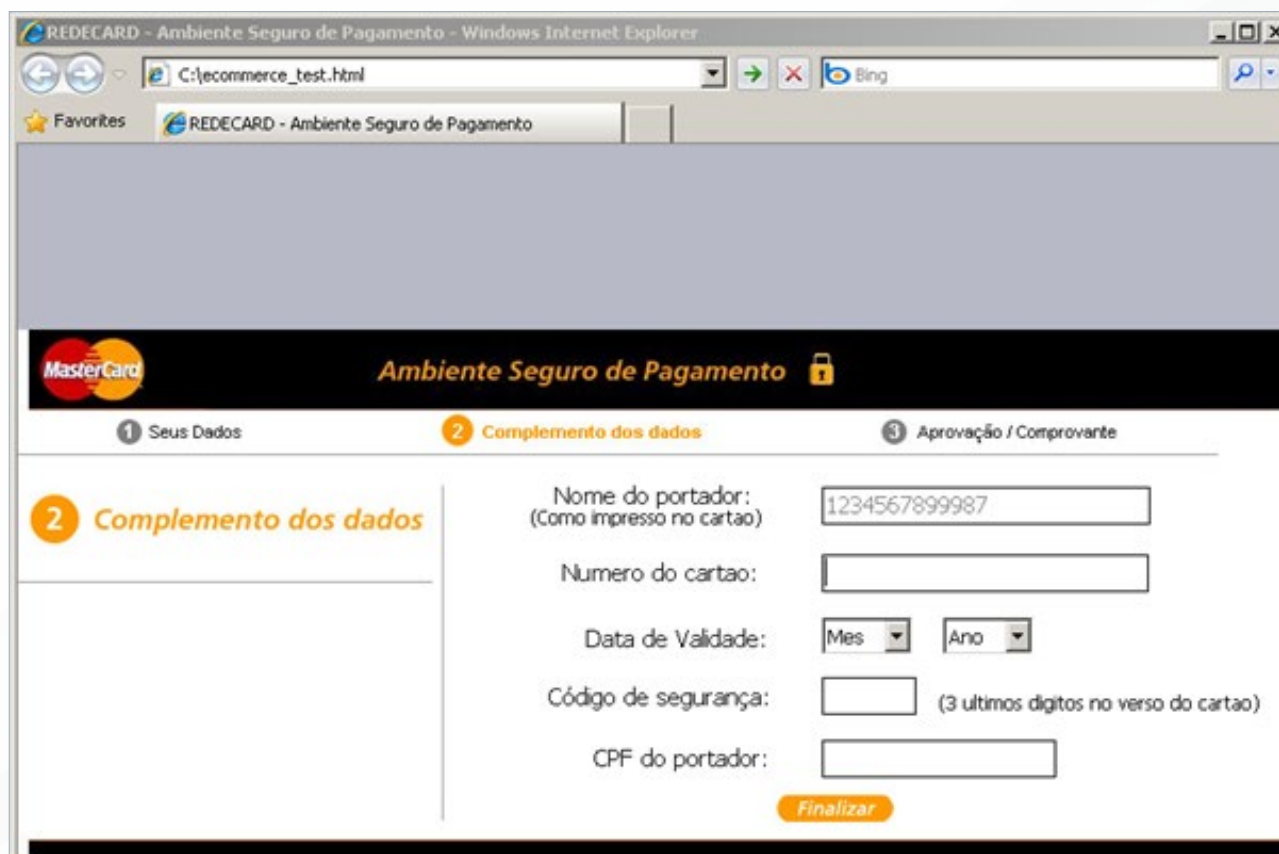
Faked PayPal injected to a blank page:



Faked PayPal (Brazilian localization) injected to blank page:



The malware is very consistent in some cases. For example, it can forge all 3 payment steps on REDECARD pages (Brazilian payment card co-operating with MasterCard, VISA, etc.).



We tried to simulate the DDE injection method on a blank HTML page with an appropriately modified <TITLE> tag, and you can see the results in the following figures (all forms and other graphics elements are created via Delphi GUI).

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
2 <HTML>
3 <TITLE>Admin Login</TITLE>
4 <BODY>
5 <!-- blank html page ready for inject -->
6 </BODY>
7 </HTML>
```



Demonstração do

Dúvidas Frequentes

Segurança

**Esqueci Minha Senha**



Fale Conosco

## Internet Banking - É o HSBC em seu Computador.

Utilize o mouse para informar sua senha no Teclado Virtual.

**TECLADO VIRTUAL**

1	2	3	4	5	6	7	8	9	0	Corrigir
Q	W	E	R	T	Y	U	I	O	P	Confirmar
A	S	D	F	G	H	J	K	L		
Z	X	C	V	B	N	M				

Contraste - +

**Veja Também**

- ▶ Meu HSBC Celular
- ▶ Meu HSBC Telefone
- ▶ Meu HSBC Caixa Automático

## Login

### .: Acesso ao Internet Banking

Digite seu usuário e sua Senha Internet.

**Dicas de Segurança**

- ✓ O seu cartão é de uso pessoal e intransferível.
- ✓ Não divulgue sua senha para desconhecidos, e em hipótese alguma anote a senha no cartão.
- ✓ Tenha cuidado ao digitar sua senha.
- ✓ Troque a senha de acesso ao Internet Banking periodicamente.

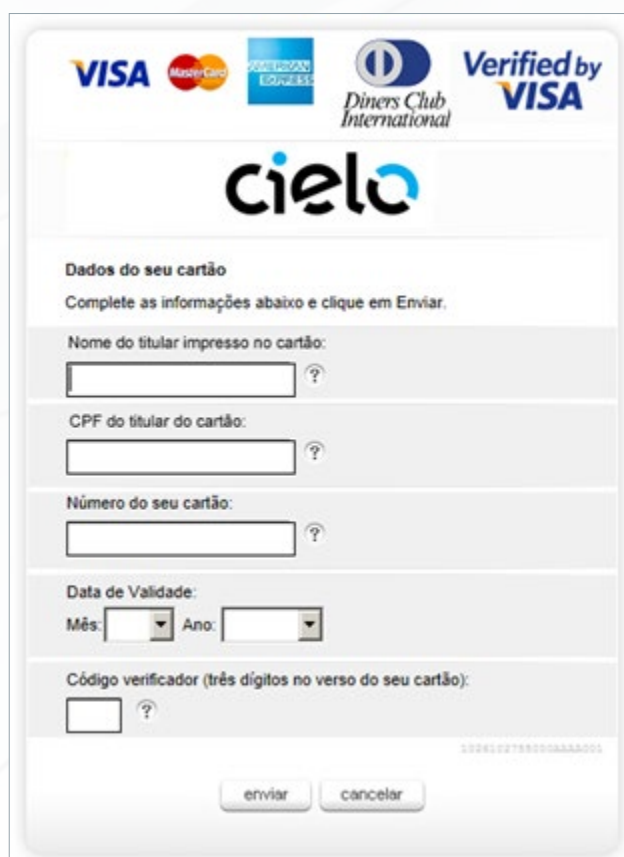
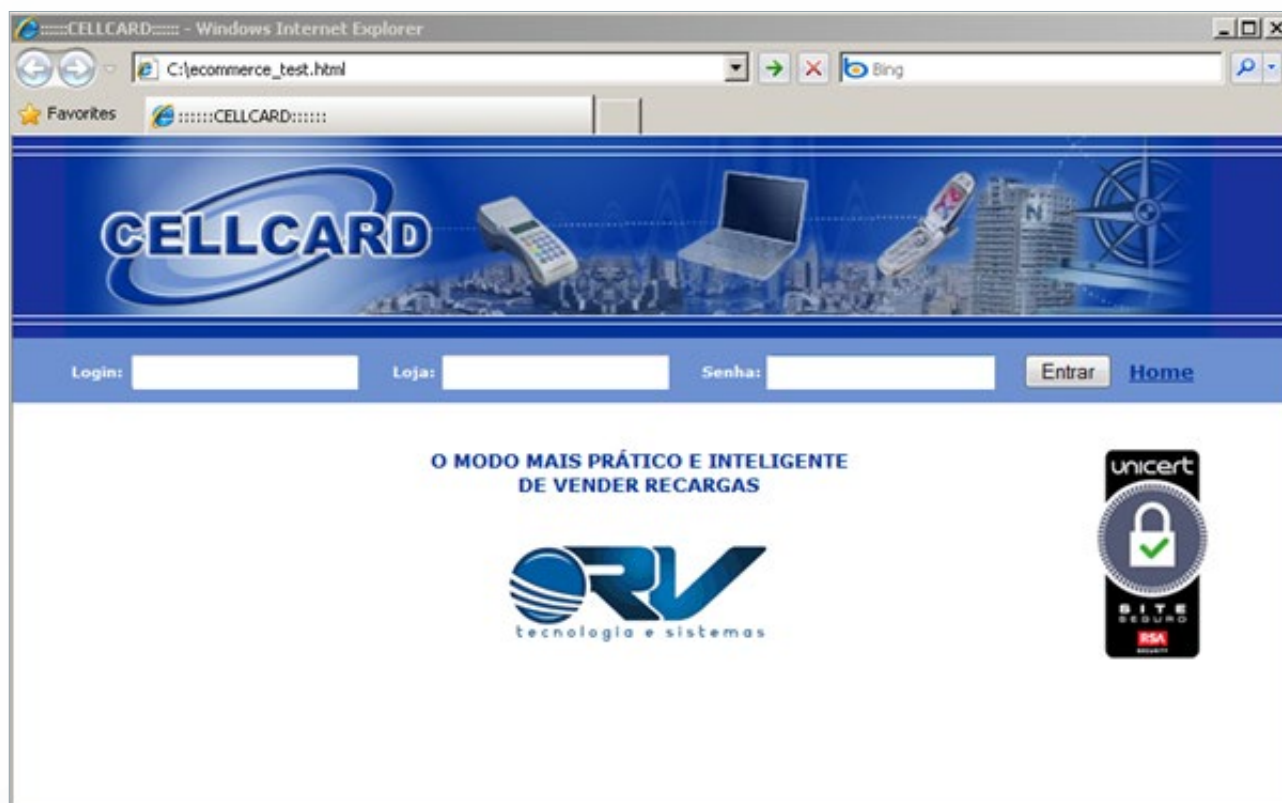
ver mais dicas

Usuário:

Senha Internet:

[Como acessar](#)  
[Esqueci minha senha](#)  
[Ainda não sou cadastrado](#)

0	8	4
9	7	6
2	3	5
1	Limpar	



**VISA** **MasterCard** **AMERICAN EXPRESS** **Diners Club International** **Verified by VISA**

**cielo**

Dados do seu cartão  
Complete as informações abaixo e clique em Enviar.

Nome do titular impresso no cartão:

CPF do titular do cartão:

Número do seu cartão:

Data de Validade:  
Mês:  Ano:

Código verificador (três dígitos no verso do seu cartão):

enviar cancelar



**Administrator's Login**

Please enter your username and password:

Userid

Password

Password 2

Login



User Name:

Password:

Login Reset

Registration Key:

Powered by SmartWin Technology eCommerce Software

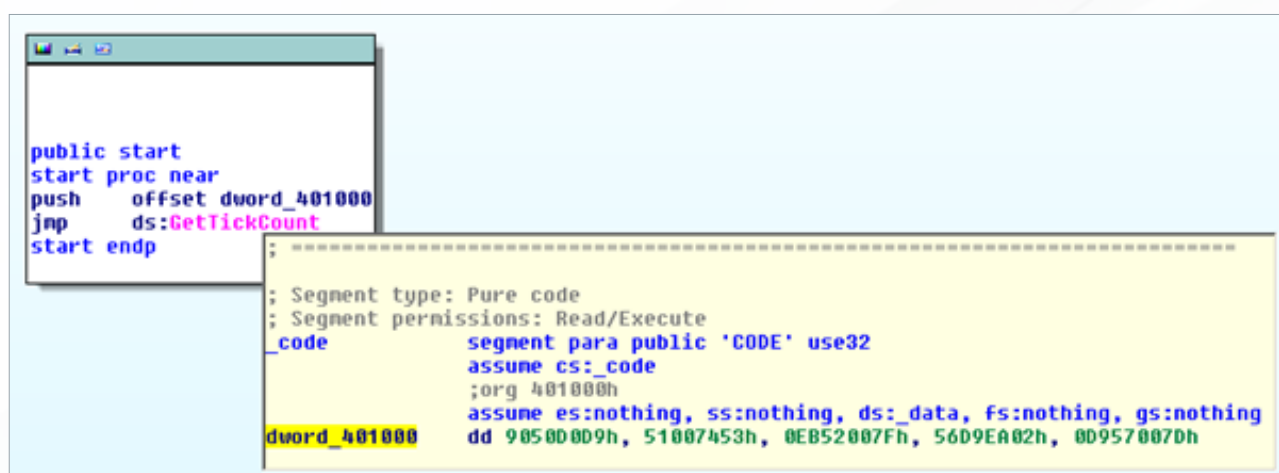
All filled data in modified forms, credentials, personal information, passwords, PIN codes, virtual keyboard hits, and other important data are immediately sent to attackers' emails.



## Reversing stuff

The whole banker malware has weak protection against reverse engineering, despite its long evolution. We found only a few security elements during the analysis, and it again shows inexperience authors.

The first simple anti-debug trick can be found right at the Entry Point. Although it is a primitive trick, it can fool an IDA disassembler and some simpler emulators.



The authors also effectively mask the API calls from the system DLLs. The code is obfuscated and complicates orientation.



All the essential texts/strings are "encrypted" using 1 byte XOR loop or custom Base64 algorithm.



After decrypting all texts we've been able to recover lists of URLs, affected <Title> tags, module settings, email templates ready for fill with stolen data, error messages, and plaintext strings for other webpage elements. We also found login credentials to attackers' emails.

The emails with the stolen credentials are not encrypted at all.



## Some info about malware creators

We have accumulated a lot of tracks that point to the banking malware's creators during the analysis, because all emails and login information are hardcoded to the malware.

Here is a list of some attackers' emails.

```
anamariabraga@email.it  
coisa_de_quem_fatura_alto_malandro@contractor.net  
enjoy.the.silence@hackermail.com  
everythingcounts@greenmail.net  
omniavincit8@graffiti.net  
umanodourado2010.3@gmail.com  
umanodourado2010@greenmail.net  
words_are_very_unnecessary@yahoo.com
```

These emails are not to be found via simple Internet searches, most probably because the authors did not use them anywhere else, so we looked for other traces. We found interesting information from WHOIS (domain registry information database).

We checked all registered domains from the digital certificates and discovered two names. After we checked the first domain connected with the malware (Omnia-vincit.com – a Latin phrase meaning "Conquers All") we found the same person as the gastechnology.org domain registrant. We were surprised by the connection between these domains. We found two contacts that match, as you can see in the picture below.

Domain Name:	OMNIA-VINCIT.COM
Registrant Name:	HERMILTON MACHADO DE MELO
Registrant Street1:	R MOACIR AVIDOS 112, ap303
Registrant City:	Vitoria
Registrant State/Province:	ES
Registrant Postal Code:	29057-230
Registrant Country:	BR
Registrant Phone:	+55.273395217
Registrant Email:	hmachadodemelo@yahoo.com

Domain Name:	GASTECNOLOGY.ORG
Registrant Name:	GAS TECNOLOGY
Registrant Street1:	R MOACIR AVIDOS 112, ap303
Registrant City:	Vitoria
Registrant State/Province:	ES
Registrant Postal Code:	29057-230
Registrant Country:	BR
Registrant Phone:	+55.8130761412
Registrant Email:	hmachadodemelo@yahoo.com
Domain Name:	G-BUSTER.ORG
Registrant Name:	PAULO RENATO REIS DE ABREU PINTO
Registrant Organization:	G-Buster
Registrant Street1:	AV PAPA JOAO PAULO I 501, APT 33 BLOCO D
Registrant City:	SAO JOSE DOS CAMPOS
Registrant State/Province:	SP
Registrant Postal Code:	12231-710
Registrant Country:	BR
Registrant Phone:	+55.6133491188
Registrant Email:	admin@g-buster.org
Domain Name:	GPSISTEMAS.NET
Registrant Name:	PAULO RENATO REIS DE ABREU PINTO
Registrant Organization:	G&P PROJETOS E SISTEMAS LTDA
Registrant Street1:	R MQ DE ITU 70, VILA BUARQUE
Registrant City:	SAO PAULO
Registrant State/Province:	SP
Registrant Postal Code:	01223-903
Registrant Country:	BR
Registrant Phone:	+55.1120597885
Registrant Fax:	+55.1120597885
Registrant Email:	paulorrdeapinto@yahoo.com

Discovered names include "Hermilton Machado De Melo" from Vitoria and "Paulo Renato Reis De Abreu Pinto" from Sao Paulo.

Two certificates were not given a domain, but according to data from the certificates we discovered these registrars (again from Sao Paulo).

```
BUSTER ASSISTENCIA TECNICA ELETRONICA LTDA - ME  
Estrada do Campo Limpo, 1198  
Sao Paulo - SP, 5777000  
http://www.bse.kit.net/  
bseseguranca@globo.com  
Tel.: 55109050, (11) 5819-3359
```

```
BUSTER PAPER COMERCIAL LTDA ME  
Sao José Dos Campos  
Sao Paulo  
Brazil  
Tel.: 55813075-2364
```

The malware includes a large number of short strings or author messages. From these strings we can deduct that the authors are fans of Depeche Mode and the X-men franchise. We also found other texts that refer to the Crime in Carson City, Nevada, or a short story by author Gabriel Garcia Marquez. One of the first messages was YOUNEEDLOVE.

```
1998XMENORIGIN  
OUR_WORDS_ARE_VIOLENCE89712  
DONT_BELIEVE_THE_TRUTH  
WORDS_ARE_UNNECESSARY  
THEY_CAN_ONLY_DO_HARM  
LET_ME_SEEW_YOU_STRIPPED  
DOWN_TO_THE_BONNE  
THE_CONSTRUCTION_OF_TIME_AGAIN  
WHATEVERHAPPENTOOURLOVE  
NEVER_GIVE_UP  
THEREISALIGHT  
THERE_IS_A_STAR_IN_THE_SKY  
I_AM_WAITING_FOR_THE_NIGHT_TO_FALL  
WEALLNEEDLOVE  
GOKRATOSGO  
WHATHAVEIDONETODESEVETHIS  
FARAWAYSOCLOSE  
ITSOVERWHENTSOVER  
AND_THEY_LIVE_HAPPILY_EVER_AFTER  
OTHERS_WILL_GET_LUCKY  
LIKE_ME_MEETING_YOU
```

## Conclusions

It is very striking that ancient technology such as DDE (introduced in 1987!) is able to avoid security features of modern browsers. The malware is checking the browser address bar and injecting the pieces of their code without a single click or permission from the user – which is not exactly a surprise, given the fact that the harm was already done by the user by letting the malicious software in.

It is also interesting that authors of this banker malware have been developing it for several years, unnoticed and without interruption. The malware is definitely not of high technical level, but it seems enough to earn authors money.

It is a classic case that even a small criminal group can develop malware from which they will benefit for years.

At the end, it is necessary to emphasize that buying the digital certificate is no problem for anybody, and the risk of a signed malware attack is very high. This is probably a little bit a fault of security community, which does not explain well that there are only two purposes for digitally signing binaries: to validate the integrity of the binary and to attribute it to the owner of the certificate. Any other assumptions made about the certificates are unfortunately wrong, as there is no way to deduct the legality of the business or even the existence of it.

AVAST Software Virus Lab advises that you carefully read the certificate information, not to download applications from untrusted webpages, and not to blindly trust every signed application.

## About AVAST

AVAST Software, maker of the world's most popular antivirus, protects over 184 million computers and mobile devices with our security applications. In business for over 25 years, AVAST is one of the oldest companies in the computer security business, with a portfolio covering everything from free antivirus for PC, Mac, and Android, to premium suites and services for business. In addition to being top-ranked by consumers on popular download portals worldwide, AVAST performance is certified by, among others, VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, and West Coast Labs.

For more information, please visit: [www.avast.com](http://www.avast.com)



**Czech republic (HQ)**  
AVAST software a.s.  
trianon office building  
budějovická 1518/13a  
140 00 prague 4  
Czech republic

**USA**  
AVAST Software, Inc.  
255 Shoreline Drive, Suite 515  
Redwood City, CA 94065  
USA

**Germany**  
AVAST Software  
Deutschland GmbH  
Otto-Lilienthal-Str.4  
88046 Friedrichshafen  
Germany

**Austria**  
AVAST Software  
Österreich GmbH  
Rosenauerstr. 50  
4040 Linz  
Austria