



Ascending the Ranks
The Brazilian Cybercriminal Underground in 2015

Forward-Looking Threat Research (FTR) Team

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.

Contents

4

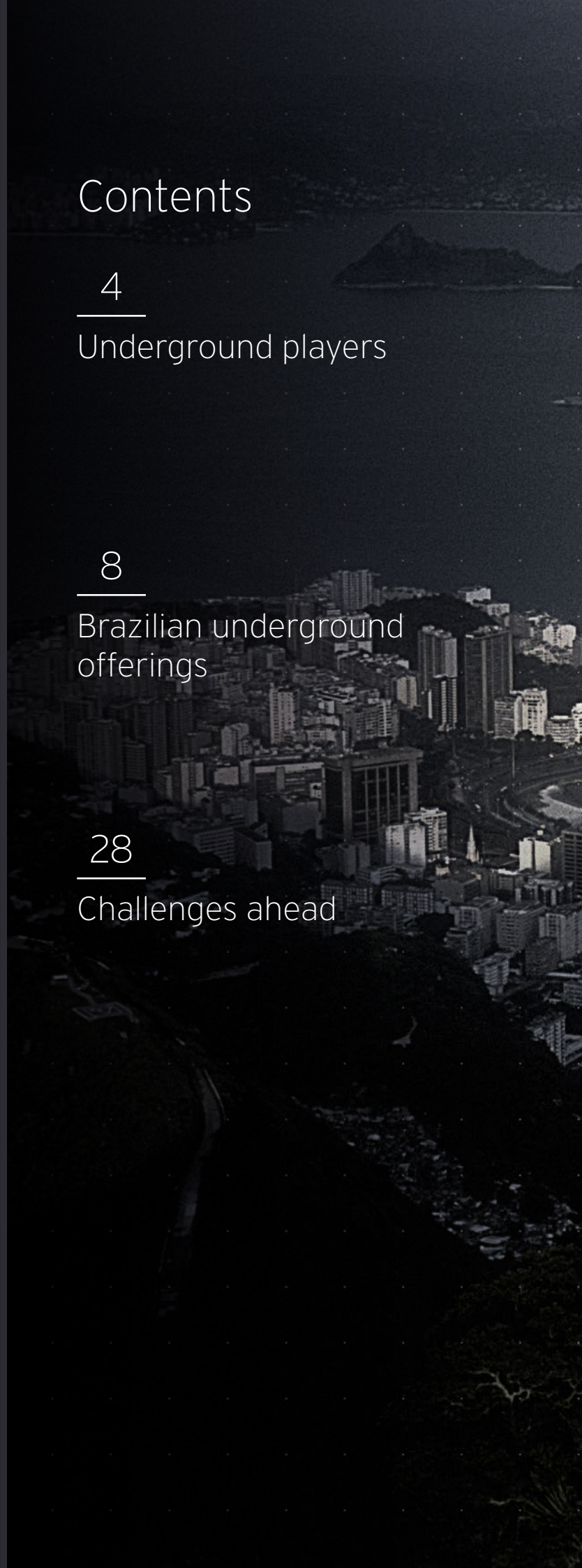
Underground players


8

Brazilian underground offerings

28

Challenges ahead





The fastest route to cybercriminal superstardom can be found in Latin America, particularly in Brazil. Any criminal aspirant can gain overnight notoriety with just a little bit of moxie and the right tools and training, which come in abundance in the country's untamed underground.

This past year, we observed an influx of new players in the scene. Most of them are young and bold individuals with no regard for the law. Unlike their foreign counterparts, they do not rely so much on the Deep Web for transactions. They exhibit blatant disregard for the law by the way they use the Surface Web, particularly popular social media sites like Facebook™ and other public forums and apps. Using online aliases on these sites, they make names for themselves, flagrantly showing off all the spoils of their own mini operations. Although they share what they know to peers, they mostly work independently, trying to outdo the competition and ascend the ranks to become the top players in their chosen fields.

Online banking is their biggest target; this makes banking malware and respective how-to tutorials prevalent. This trend remains consistent with what we reported two years ago¹. But since then, new offerings have also sprouted, including localized ransomware and personally identifiable information (PII)-querying services. Illegal goods that were only peddled in Brazil's backstreets have likewise crossed over to the underground. Anyone can now purchase counterfeit money and fake diplomas online.

The brazenness of cybercriminal operations should come as no surprise. Brazilian law enforcement agencies already have a lot on their plate; budding criminals online are only additions to their list of challenges. Although they have started investing in the fight against this growing problem, will their efforts be enough to at least slow down its pace?

A high-angle, close-up photograph of a person's hands typing on a laptop keyboard. The scene is dimly lit, with the primary light source being the laptop screen, which is out of focus in the background. A large, semi-transparent circular graphic with a grid-like border is centered over the hands. Within this circle, there is a red rectangular box containing the text 'SECTION 1' and the title 'Underground players' below it.

SECTION 1

Underground players

Underground players

Brazilian cybercriminals operate either solo or in groups, though more often than not, they prefer to work individually. They can be classified under two main categories—developers and operators.

Developers are educated individuals who turned cybercrime into a lucrative job. They aid their fellow cybercriminals, in a way, by providing malware that they themselves created. Unlike cybercriminals in other regions, they do not use the Deep Web as much. As stated earlier, Brazilian cybercriminals have little to no regard for law enforcement. Their audacity allows them to take their operations to the Surface Web. They use publicly accessible social networking platforms like Facebook, Twitter™, YouTube™, Skype™, and WhatsApp™, as well as Internet Relay Chat (IRC), TorChat, and forums for business transactions.

Operators, meanwhile, purchase malicious wares from developers and try to profit by using them against certain targets.

Developers

Typical developers are young and have a working knowledge of creating software. More often than not, they are students who picked up their skills in school. Ease of access to malware training and tools, along with their current financial circumstances, could be some of the factors that drove them to start venturing into the underground. The weakness of Brazil's laws against cybercrime also made them bold enough to even publicly advertise their success.

One such developer is the notorious 20-year-old Lordfenix² whom we profiled in June 2015. This computer science student was able to build more than 100 banking Trojans that can bypass Brazilian banks' security measures. This has earned him a reputation as one of the country's top banking malware creators. He supposedly started developing his own malware when he was still in high school and remains an active underground player to date.

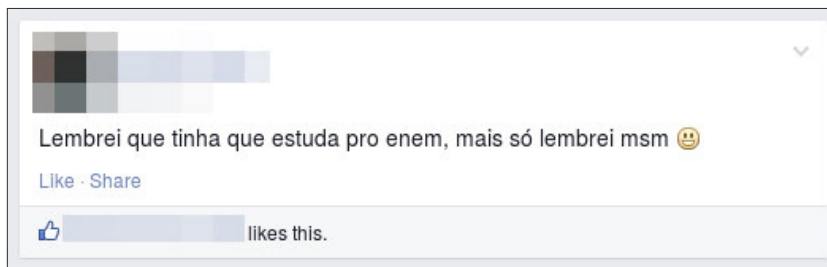


Figure 1: Lordfenix telling his friends he has to study for the Exame Nacional do Ensino Médio (ENEM), which is the equivalent of the SAT in the United States (US)

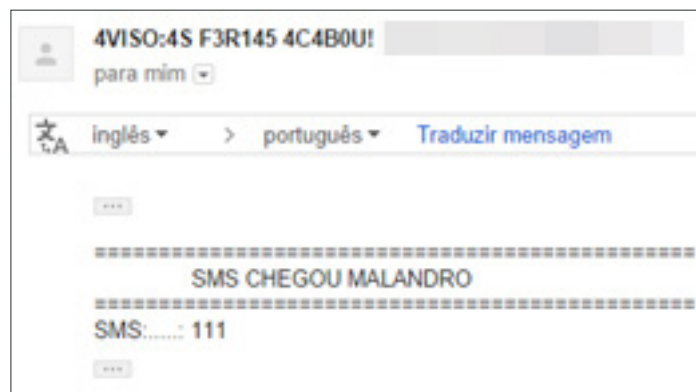


Figure 2: Message with the subject, "Warning: Vacation has ended," that Lordfenix sends to his malware operators; this could mean he can work more on his malicious creations



Figure 3: Lordfenix's post boasting of his Trojan's success

We investigated another professional developer known as “Antrax” who publicly posted a video advertising a banking Trojan that he created. He remains an active underground player to date. A screen capture of his computer shows that he uses disk partitions, which amateur computer users may not know. Particularly interesting was his TRABALHO (Portuguese for “work”) partition, which apparently contained several directories for malicious creations like keyloggers, crypters, and exploit kits.

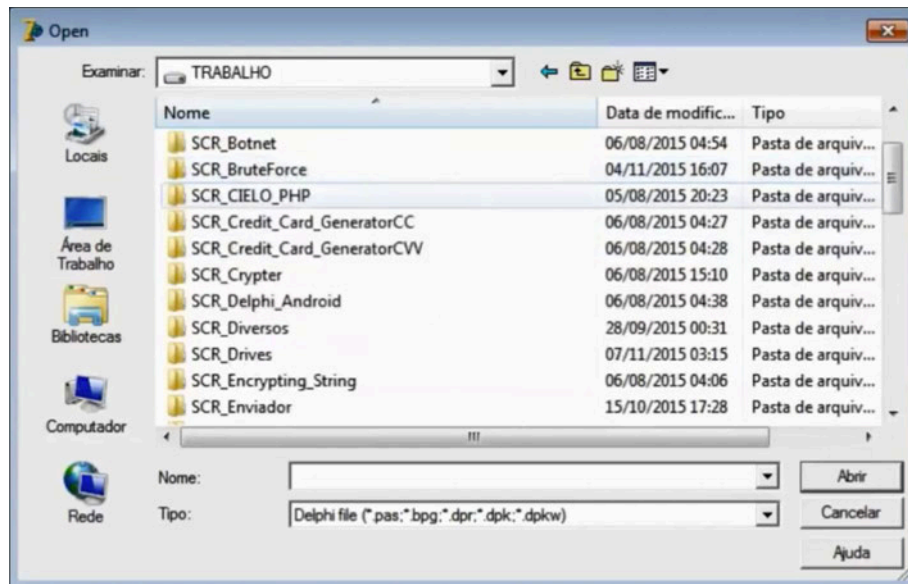


Figure 4: Different directories in Antrax’s TRABALHO partition (Note that this was captured from a publicly accessible video.)

Operators

Unlike developers who sell their creations to fellow cybercriminals, operators interface with actual victims. They buy malware from developers or rent cybercriminal infrastructure via the crime-as-a-service (CaaS) business model. Their modus operandi vary, depending on how they use the wares they purchase. The cybercriminal behind FighterPoS³ is an operator. Law enforcement agencies can more easily catch operators but have a harder time tracking down malware developers.

In August 2015, the Goiás State Civil Police arrested 20 people who were involved in bank card cloning and other kinds of fraud⁴. Those arrested reportedly stole a total of US\$200,000.



SECTION 2

Brazilian underground offerings

Brazilian underground offerings

The Brazilian underground is still heavily congested with banking malware, which could be largely attributed to the continued popularity of online banking⁵ in the country. A few additional offerings like multiplatform and local-flavored (made in Brazil and uses Portuguese) ransomware, modified Android™ apps, and PII-related services. Tutorials remain popular since they help cybercrime newbies learn important tricks of the trade. Some trainers could also be using these courses to recruit gang members.

Typical criminal modus operandi seen in the backstreets of Brazil have gone digital and are currently making waves in the country's underground market. We have, for instance, seen fake diplomas and counterfeit money for sale.

Latest market entrants

Ransomware

Ransomware's massive success and continued prevalence worldwide⁶ make them a very important tool in any cybercriminal's arsenal. It was really just a matter of time before Brazilian cybercriminals created their own version of the malware, given their effectiveness.

For US\$3,000 or 9 BTC, cybercriminals can use an unlimited number of multiplatform ransomware from the seller's arsenal in a span of a week. These threats run on Windows®, Linux®, Android, iOS™, and OS X™ devices. They encrypt .JPG, .PNG, .GIF, .PDF, .TXT, .SQL, .DOC, .XLS, .HTML, .HTM, .XHTML, .BMP, and .PHP files using Triple Data Encryption Standard (DES) (3DES), Advanced Encryption Standard (AES), DES, or Rivest Cipher 4 (RC4).

Ransoware FileCrypter Rodando Windows , Android ,IOS,OSX, Linux.

 Preço USD:3.000.00 ou 9 BTC. bitcoin. Por semana Aluguel Semanal.
 Encripta Todos Arquivos do Sistema , Seja as extensões , jpg,png,gif,pdf,txt,sql,doc,xls,html,htm,xhtml,sql,bmp.php que estiver no sistema
 Metodos de Encriptação 3DES AES DES RC4 .
 Resgate via Bitcoin .
 Inclui Painel Completo Mostrando Quantidades de Pcs Infectados , Resgatados com Pagamentos , Não Resgatados E Valor Total Dos Resgates .

Figure 5: For 9 BTC per week, cybercriminals can use the ransomware of their choice for attacks

In one ad, a seller even noted that the piece of FileCrypter ransomware includes a full panel showing the number of devices it infected, details on the users who paid the ransom, and the total amount he has received as payment so far. Paying the ransom doesn't ensure that those who gave in won't be targeted again, given that the cybercriminals knew they have the capacity to pay. The fact that victims were asked to pay in bitcoins (BTC) also suggests the increasing popularity of the cryptocurrency in the country.

Modified Android apps

Modified Android apps also recently figured in the Brazilian underground. These have been configured to pay for prepaid credits with stolen credit card credentials. Even better, users weren't even required to key in additional information, including the Credit Verification Value (CVV) number and billing address, to complete transactions. These modified apps' Android application packages (APKs) can be obtained from underground forums.



Figure 6: Post advertising modified Android apps that allowed users to buy prepaid credits with stolen credit card credentials

This underground offering's emergence could be attributed to the high mobile device penetration rate in Brazil (142% as of April 2015)⁷. Most Brazilians even accessed the Web via mobile devices instead of computers. Even organizations and companies encouraged customers to use mobile devices for all kinds of business transactions.

PII-querying services

Cybercriminals in Brazil have also started offering services that involved stealing victims' PII that they can then sell to others for 0.015 BTC (US\$6.81)*. Some cybercriminals even claimed to have access to vehicle registration plate databases. The stolen PII could be from hacked or compromised databases like CadSUS (Brazil's national health card system). In some cases, government employees have been reported guilty of selling access to national databases.



Figure 7: Ad touting stolen PII for sale

Buyers of stolen PII can easily register domains and send out spam for various malicious purposes.

* Currency exchange rate as of 16 December 2015 was used throughout this paper (1 BTC = US\$461.26)

Brazilian underground staples

Malware

Banking Trojans continued to heavily figure in the Brazilian underground. Most of the banking malware seen today continue to have ties to Brazil (often made or distributed by locals or residents). Several factors could have led to this like the high online banking adoption rate in the country. More than 40% of Brazil's population banked online as of 2014. Brazilians would rather use their computers or smartphones to check their account balances online more than physically go to their bank branches or call designated hotlines⁸.

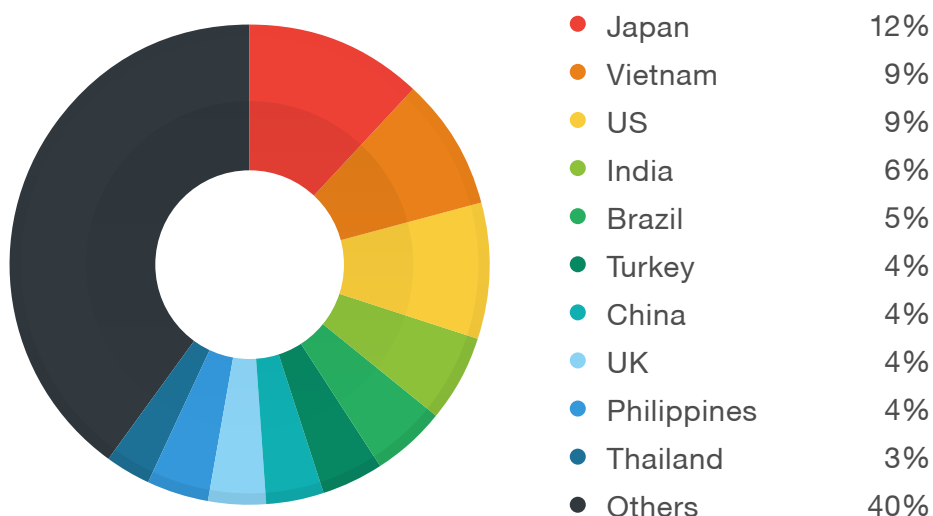


Figure 8: Brazil accounted for 5% of the total number of online banking malware detections in the third quarter of 2015⁹

Based on our research, some banking malware were capable of locking users' device or computer screens after security checks have been made while attackers illegally transferred money to their own accounts in the background. This capability gave law enforcement agencies a harder time tracking the responsible cybercriminals.

KAISER malware

KAISER malware can bypass Sicredi's (a Brazilian credit union) time-based tokenization system, among others. They can also put customers of Banco do Brasil, Itaú, HSBC, Santander, and Bradesco at great risk. Operators usually sent out KAISER-laden spam to intended recipients. Every time users of infected systems visited target banks' sites, KAISER logged their keystrokes. Cybercriminals then obtained victims'

account numbers for a variety of nefarious purposes.

KAISER also opened fake windows (on top of the real ones) so the cybercriminals could obtain the victims' tokens. When we analyzed a KAISER sample, we found a fake window (with a fake form) that asked victims to key in their tokens when asked by (supposedly) Sicredi. Filling in the said form sends the token to the KAISER operator who then freezes the victim's device or computer screen while transferring as much money as possible to their own accounts.

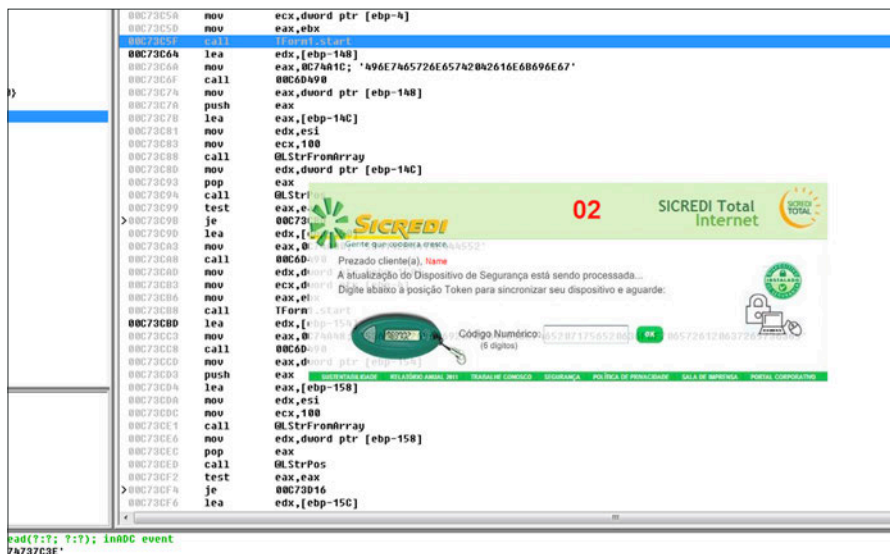


Figure 9: Fake form that appears on KAISER-infected systems when Sicredi customers are asked to input their tokens

Proxy keyloggers

Proxy keyloggers are known for redirecting victims' browsers to phishing pages every time they access target banks' official sites on infected computers. These have a remote desktop access feature that allowed cybercriminals to access and even control victims' screens. Certain Proxy variants even had Proxy Auto Configuration (PAC) scripts that let them select what proxy servers to use (preferably those that can't be traced back to the operators).

We found a post selling a Proxy variant that had a remote access feature and came with a customizable crypter for R\$5,000 (US\$1,279.02)**. Buyers can log keystrokes from as many as 15 sites, including those of PayPal and HSBC. They even get access to 24 x 7 support services.

** Currency exchange rate as of 16 December 2015 was used throughout this paper (US\$1 = R\$3.91)

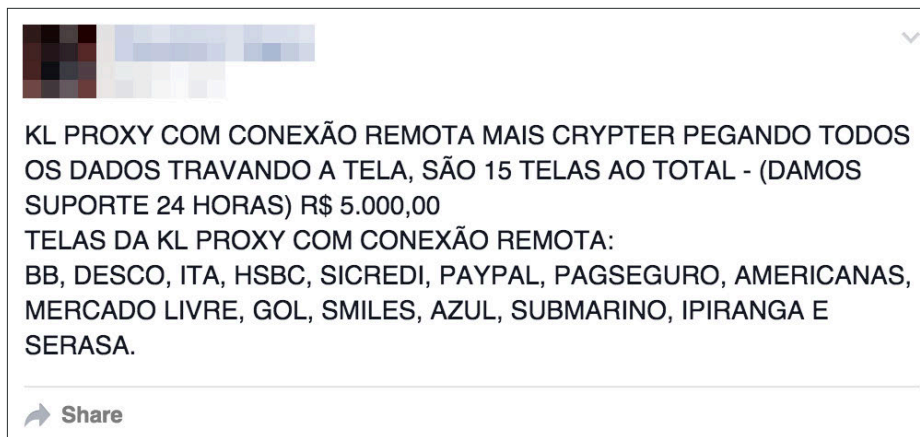


Figure 10: Post promoting Proxy keyloggers

Remota keyloggers

Remota (Brazilian for “remote”) keyloggers have the ability to fake all kinds of browser windows every time users access target bank sites on infected computers. And for R\$2,000 (US\$511.61), operators even get full support and updates each week.

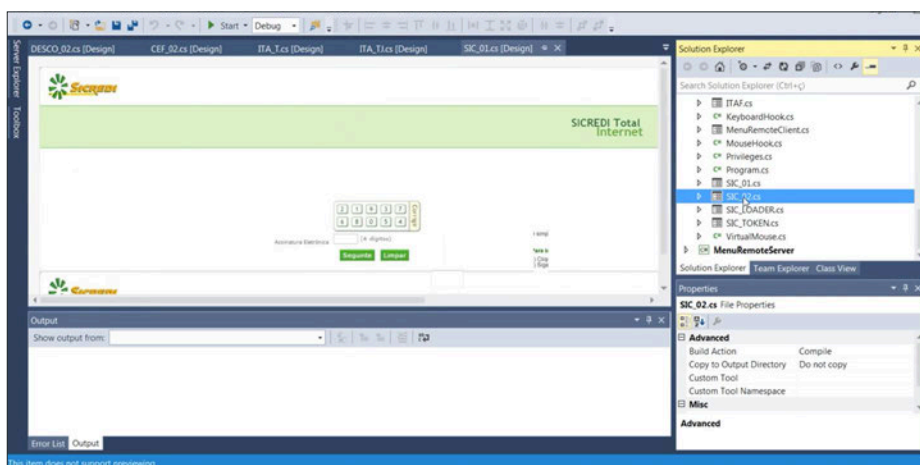


Figure 11: Remota keyloggers’ features

DNS changers

Full source codes for Domain Name System (DNS) changers are sold for R\$5,000 (US\$1,279.02) in the Brazilian underground. Note that prices may vary, depending on the seller’s level of expertise, the programming language used, and infection routines. Offerings like these come in a .ZIP file with detailed instructions for use and malware samples when bought.

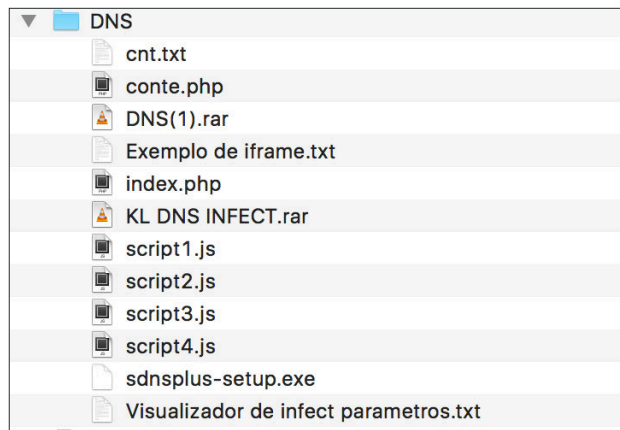


Figure 12: Sample DNS changer package sold underground

DNS changers redirect victims to phishing pages every time they access a target site. These allowed cybercriminals to steal victims' site credentials (usernames, passwords, etc.). DNS changers can not only affect computers though, as we've seen them set their sights on home routers¹⁰ in May 2015. Most of the DNS changers developed in Brazil are written in JavaScript though compiled versions are also available underground.

File Name	Modified Date	Size
Minha_DNS	Nov 18, 2015, 3:07 AM	997 KB
contado...dificado	Nov 25, 2015, 4:53 AM	9 KB
acessos.txt	Dec 2, 2014, 10:50 PM	Zero bytes
cont.php	Dec 2, 2014, 1:52 AM	430 bytes
contador.php	Dec 3, 2014, 12:32 AM	1 KB
index.php	Apr 10, 2008, 1:26 AM	182 bytes
logar.php	Apr 10, 2008, 1:26 AM	236 bytes
menu.php	Dec 2, 2014, 1:49 AM	555 bytes
rdp.php	Dec 2, 2014, 1:48 AM	139 bytes
contador.php	Nov 25, 2014, 9:45 AM	1 KB
contador.rar	Dec 2, 2014, 12:45 PM	6 KB
Services.~dpr	Dec 3, 2014, 9:02 PM	13 KB
Services.cfg	Jan 3, 2015, 11:03 PM	434 bytes
Services.dof	Jan 3, 2015, 11:03 PM	2 KB
Services.dpr	Jan 3, 2015, 11:03 PM	13 KB
Services.exe	Jan 3, 2015, 11:03 PM	603 KB
Services.ico	Dec 3, 2014, 12:51 AM	66 KB
Services.res	Dec 3, 2014, 12:52 AM	66 KB
support.ini	Jan 3, 2015, 10:49 PM	25 bytes
WbemS..._TLB.pas	Jan 3, 2015, 11:01 PM	207 KB
Win.RES	Oct 6, 2013, 6:42 PM	1 KB

Figure 13: Sample contents of a compiled DNS malware package sold underground

Cybercrime training

Carding

We found an ad for a three-month-long carding training in the Brazilian underground. This includes lessons on creating malware, setting up botnets, and obtaining victims' credit card data, among others. In the first month, trainees learn how to access a database containing stolen credit card credentials. They will then be taught what to do when a purchase made with a stolen credit card is approved and if their money mules fail. In the second month, trainees learn how to (physically) clone cards and create banking Trojans (Proxy and Remota variants, along with other banking Trojans with reverse-connection capabilities). And in the last month, they learn to create crypters using AutoIt, Visual Basic® 6.0, and Visual Basic .NET (VB.NET) as well as set up a ZeuS or Solar botnet, among others. For R\$300 (US\$76.74) paid via PagSeguro (a PayPal-like service), cybercriminal wannabes and newbies can learn to create their own malware and phishing pages to steal from victims aided by local money mules.

Peddling cybercrime tutorials must be lucrative, as this is the second time we've seen this particular instructor offer carding training using updated modules.

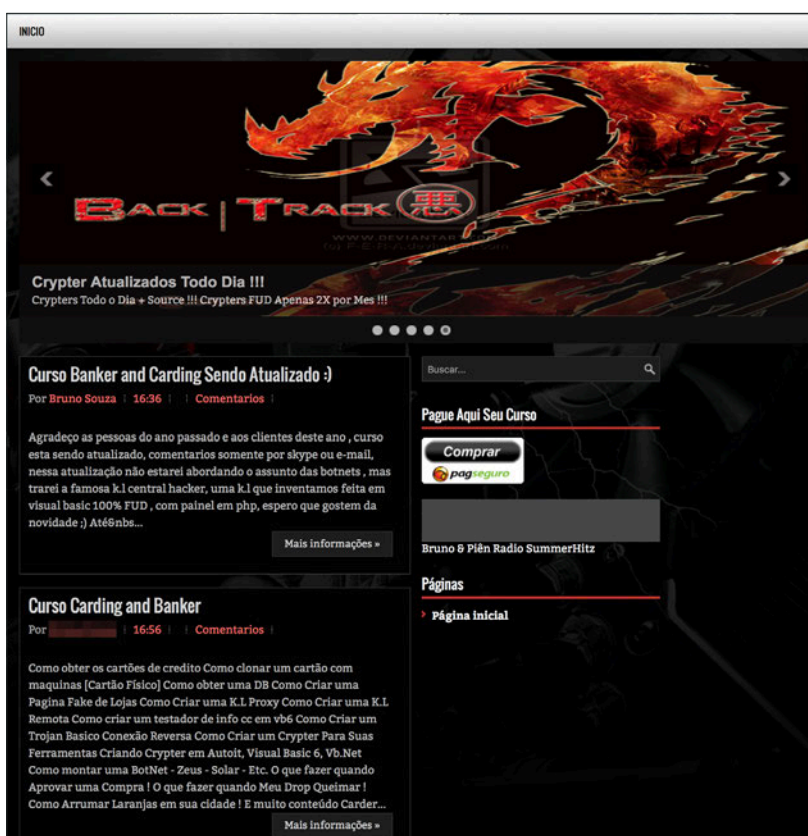
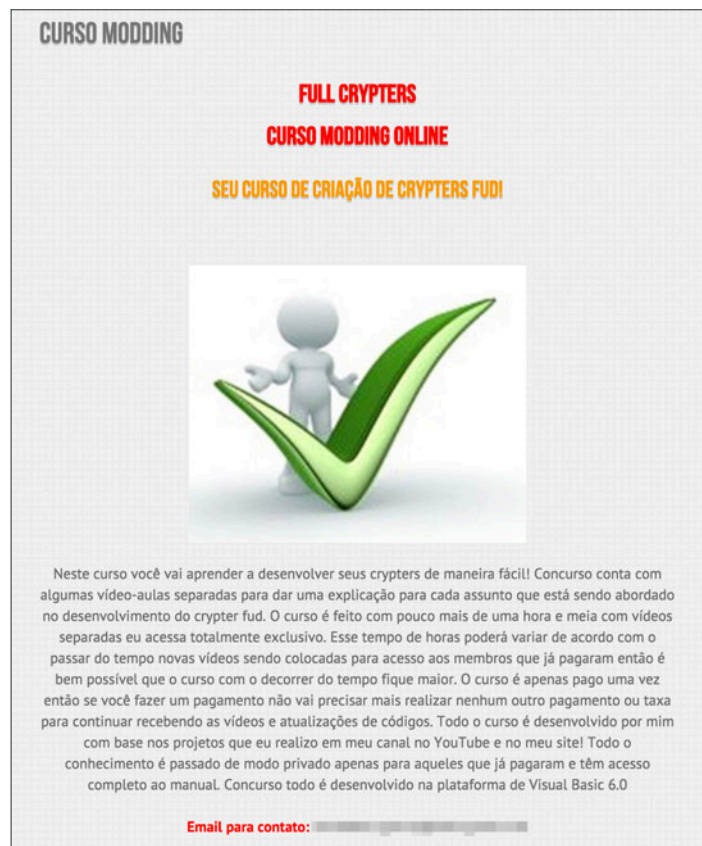


Figure 14: Site where cybercriminal wannabes and newbies can avail of carding training

Trainees also get access to virtual private server (VPS) hosts, tools, and tutorials collected from various underground forums.

Crypter programming

For as little as R\$200 (US\$51.16), cybercriminals can already avail of crypter programming training with online support via Skype. Trainees are also taught how to make their crypters fully undetectable (FUD) using Visual Basic 6.0. Trainees also receive a 1.5-hour-long video as supplementary material, along with free access to updated videos.



CURSO MODDING

FULL CRYPTERS
CURSO MODDING ONLINE

SEU CURSO DE CRIAÇÃO DE CRYPTERS FUDI

Neste curso você vai aprender a desenvolver seus crypters de maneira fácil! Concurso conta com algumas vídeo-aulas separadas para dar uma explicação para cada assunto que está sendo abordado no desenvolvimento do crypter fud. O curso é feito com pouco mais de uma hora e meia com vídeos separadas eu acesso totalmente exclusivo. Esse tempo de horas poderá variar de acordo com o passar do tempo novas vídeos sendo colocadas para acesso aos membros que já pagaram então é bem possível que o curso com o decorrer do tempo fique maior. O curso é apenas pago uma vez então se você fazer um pagamento não vai precisar mais realizar nenhum outro pagamento ou taxa para continuar recebendo as vídeos e atualizações de códigos. Todo o curso é desenvolvido por mim com base nos projetos que eu realizo em meu canal no YouTube e no meu site! Todo o conhecimento é passado de modo privado apenas para aqueles que já pagaram e têm acesso completo ao manual. Concurso todo é desenvolvido na plataforma de Visual Basic 6.0

Email para contato: [REDACTED]

Figure 15: Post advertising a crypter-modification course offering

Credit card-related goods

Online shop administrator panel access

Access to compromised online shop administrator panels can also be bought in the Brazilian underground. These panels give cybercriminals access to the shop customers' credit card data. Cybercriminals can steal as many as 40–170 sets of credit card credentials each day. Buyers are charged depending on how many sets of credentials they wish to gain access to.

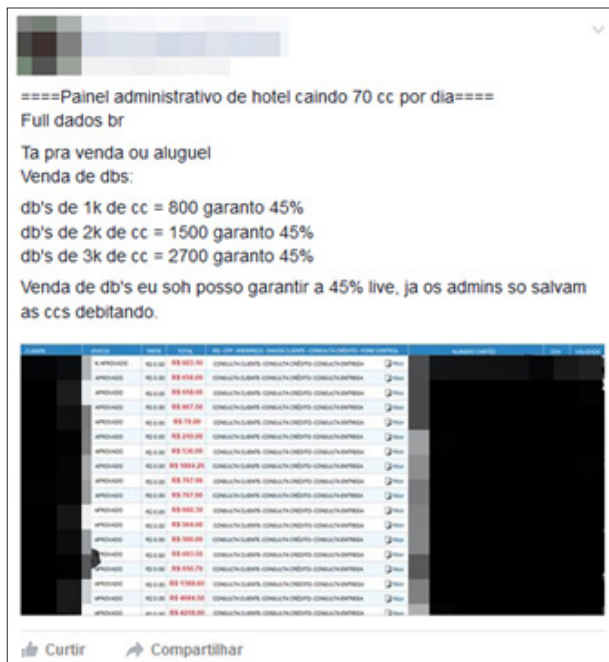


Figure 16: Post advertising access to compromised online shop administration panels

We were able to contact a seller who sold 21-day (three-week) access to compromised panels that gave 40 sets of credit card credentials per day for R\$300 (US\$76.74). For 14-day (two-week) access to 70 sets of credit card credentials per day, buyers would need to shell out R\$500 (US\$127.90). The seller even offered 20-day access to 170 sets of credit card credentials per day at a special discounted price of R\$1,000 (US\$255.80).

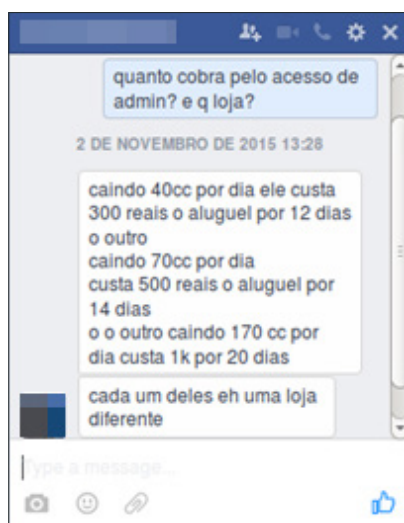


Figure 17: Conversation with a seller of access to compromised online shop administration panels

Stolen credit card credentials

Cybercriminals obtain credit card credentials via phishing, compromising banking or other payment-related sites, and distributing banking Trojans. They can also get such information from modified PoS skimmers that get installed in legitimate business establishments.

Offering	Price
10 sets of credit card credentials	R\$200 (US\$51.16)
20 sets of credit card credentials	R\$400 (US\$102.32)
50 sets of credit card credentials	R\$700 (US\$179.06)

Table 1: Credit card credential offerings with their prices

LUCAS InfoCC

Aprovações 40%

AS MELHORES INFOCC DO MERCADO

10 CC FULL	R\$ 200,00
20 CC FULL	R\$ 400,00
50 CC FULL	R\$ 700,00

NOME
RG
CPF
GARANTIA DE DEBITO

Trampo Certo Pelo Certo
TODAS TESTADAS E DEBITANDO.

Share

likes this.

Give Feedback

Sponsored

CREATE AD

TAM Fidelidade e Multiplus

Resgate passagens aéreas
tam.com.br
Transfira os pontos dos seus cartões de crédito para resgatar passagens aéreas

Figure 18: Post advertising stolen credit card credentials for sale

Credit card number generators

Though the results given out by credit card generators are not 100% reliable, these are still sold underground. Credit card number generators use specific algorithms that allow them to generate possible credit card numbers. Their prices depend on how many credit card numbers they can produce. Again, the end results are not 100% reliable and, as such, may not be effectively used to make online purchases.

Offering	Price
Card generators that give out 50 credit card numbers	R\$100 (US\$25.58)
Card generators that give out 100 credit card numbers	R\$200 (US\$51.16)
Card generators that give out 150 credit card numbers	R\$300 (US\$76.74)

Table 2: Credit card number generators sold underground



Figure 19: Post advertising generated credit card numbers for sale
(Note that this means the numbers did not come from stolen credit card databases.)

PoS skimmers

As in the Chinese underground¹¹, cybercriminals in Brazil also sold PoS skimmers. These are usually based on Verifone VX 680 machines and cost R\$8,000 (US\$2,046.43). Cybercriminals modified legitimate PoS terminals so they can steal the information stored in the magnetic stripe of all of the credit cards swiped on these. We've even seen gripper¹² (a cybercriminal) sell mass-produced ATM and PoS skimmers way back in 2014.



Figure 20: Post advertising PoS skimmers for sale



Figure 21: PoS skimmers for sale

The particular model sold (VX 680) has a triple-track magnetic stripe card reader, smart card (chip-and-personal identification number [PIN]) reader, and a PIN pad. It also has various communication features (via Bluetooth®, Wi-Fi, or 3G). Depending on the technique used to modify the PoS terminal (via firmware or hardware modification), cybercrooks are able to receive stolen credit card data either over Bluetooth or by having physical access to the machines.

Pulling off fraud via modified PoS terminals requires the help of an insider who needs to install them in place of legitimate devices. The insider will also help the cybercriminals retrieve the stolen data from modified terminals. The credit card data they obtain can then be used for cloned cards.

Modified smart card readers and writers

Modified Europay, MasterCard, and Visa (EMV) card readers¹³ are commonly sold in the Brazilian underground. In a November 2014 investigation, Brazilian police officers arrested 10 individuals who were involved in related fraud cases that cost victims more than R\$3.5 million (US\$895,313.23)¹⁴. Part of the cybercriminals' modus operandi was convincing waiters of exclusive restaurants to use maliciously modified PoS terminals for credit card payments. These waiters were given R\$1,000 (US\$255.80) each to act as accomplices. The modified terminals had Bluetooth transmitters that the cybercriminals accessed later on to obtain the stolen data. That same month, several US citizens' chip-and-PIN credit cards¹⁵ were cloned and used for fraudulent purchases after travelling to Brazil, leading us to think that the country's carders are good at their chosen fields of expertise.

Credit card transaction approval services and training

Credit card fraud doesn't stop at data theft. After getting their hands on stolen credentials, cybercriminals need to work with peers who are experts at getting transactions made with stolen credit cards approved. Some of these service providers help customers use stolen credit card credentials to buy goods online. They even provide customers physical addresses where they can have the goods bought delivered. Some sell the goods to unknowing customers at only 30% of the usual goods' prices. Any cybercriminal willing to pay R\$1,300 (US\$332.54) can avail of approval services, which usually include technical support via WhatsApp or Skype.

The image is a screenshot of a WhatsApp chat post. At the top, it says 'PROMOÇÃO DE SABADO - 31/10' and 'TODAS AS APROVAÇÕES NESSA DATA SERÁ COBRADO APENAS 30% VALORES ATÉ 1300,00 DROP VIRGEM INTERESSADOS IMBOX'. Below this is a yellow banner with 'Equipe Edmar Araújo' and 'APROVAÇÕES'. The post lists various items for sale with prices in Brazilian Reals (R\$):

Category	Item	Price (R\$)
MOTOROLA	Moto E	200,00
	Moto G2	250,00
	Moto G3	350,00
	Moto X3 Play	600,00
TELEVISÕES	32" LED	350,00
	32" SMART	500,00
	40" LED	550,00
	40" SMART	650,00
GAMES	Xbox 360	280,00
	Nintendo Wii	350,00
	PS3	500,00
SAMSUNG	A5	350,00
	A7	450,00
	S5	430,00

At the bottom, there are contact details: a WhatsApp icon with the number '(34) 9251-8253' and a Telegram icon with the handle 'edmar.araujo7082'.

Figure 22: Post advertising the sale of goods bought with stolen credit cards

Apart from actual services, training to help other cybercriminals get fraudulent credit card purchases approved is also available. Trainees learn how to steal credit card credentials and even monetize their loot.

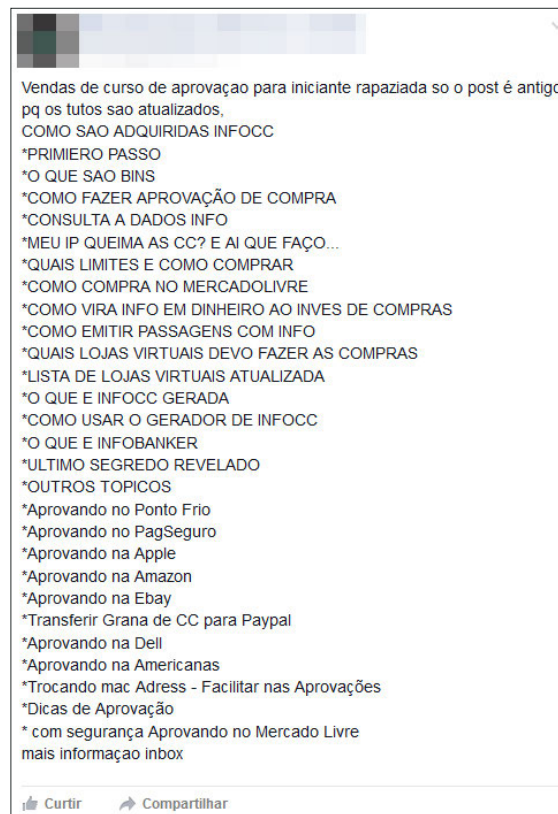


Figure 23: Post advertising fraudulent credit card transaction approval training

Approval trainees learn how to steal credit card numbers, get fraudulent purchases (on Pontofrio, PagSeguro, Apple® Store, Amazon™, eBay®, Dell, and MercadoLibre) approved, query databases, mask their Internet Protocol (IP) addresses when they use stolen credentials for online purchases, determine the available balances on stolen cards, monetize stolen card data (buy plane tickets for reselling), and generate infocc data; what bins are and InfoBanker is; and which shops they can easily buy goods from with stolen cards.

Fake documents and counterfeit money

Street crimes like selling fake documents and counterfeit money have gone online. This trend could be attributed to socioeconomic factors like widespread poverty and illiteracy. As of October 2015, Brazil's inflation rate was 9.93%¹⁶.

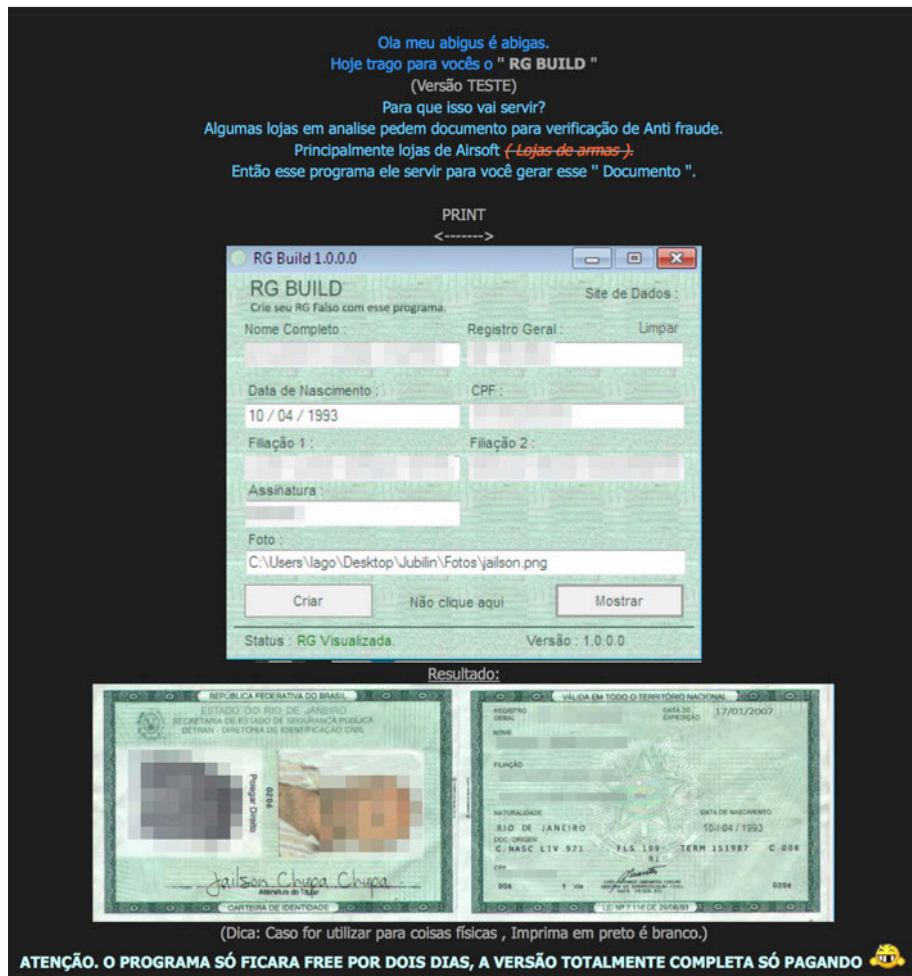


Figure 24: Fake identification (ID) makers' products sold underground

Fake diplomas

Brazil's current educational system¹⁷ somehow contributes to the lack of professionals in the country. Despite the fact that illiteracy in the country has decreased, at least 38% of Brazil's undergraduates are still considered "functionally illiterate." It's no wonder then why fake diplomas (probably for employment purposes) have now figured underground. These are sold for R\$300 (US\$76.74) each, including shipping fee. Some counterfeit money sellers even offer free shipping for purchases comprising more than 200 bills.

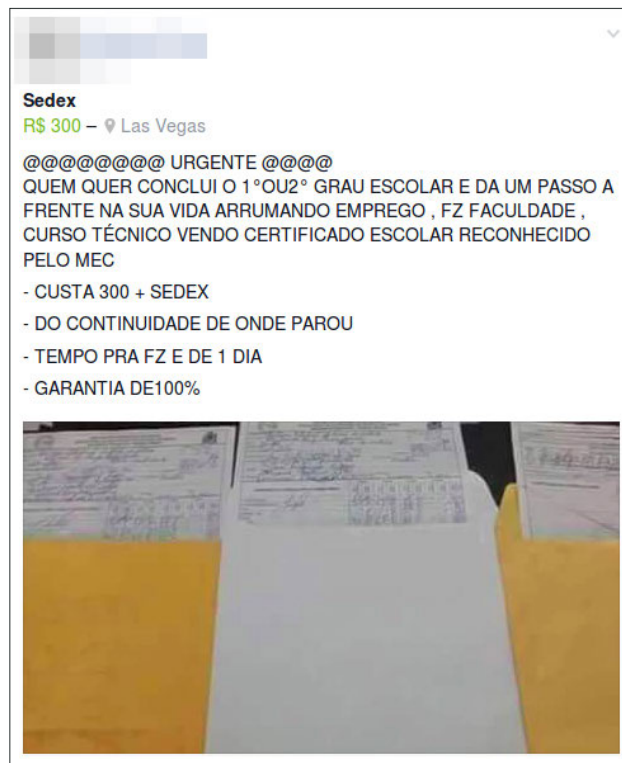


Figure 25: Fake diplomas sold underground

Counterfeit money

Counterfeit R\$10, R\$20, and R\$50 bills are sold in the Brazilian underground.

Offering	Price
R\$750 worth of counterfeit bills	R\$100 (US\$25.58)
R\$1,500 worth of counterfeit bills	R\$200 (US\$51.16)

Table 3: Prices of counterfeit money sold underground

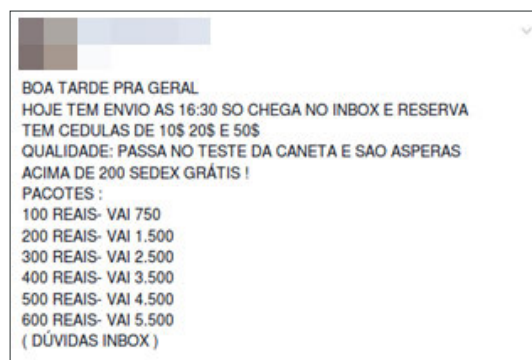


Figure 26: Post advertising counterfeit money for sale



Figure 27: Counterfeit money with the seller's name posted online

Cybercriminals in Brazil are quite brazen. They don't care if law enforcement agencies see their names posted online in relation to illegal activities.

Other illicit offerings

Internet and CATV access bump-up services

Cybercriminals who have access to the networks of Internet service providers (ISPs) and cable television (CATV) operators, for instance, sell bump-up services to customers who wish to increase their access speeds or privileges. They can speed up their Internet access or watch more shows on CATV for a price lower than what the legitimate service providers usually ask for (R\$150 [US\$38.37]).

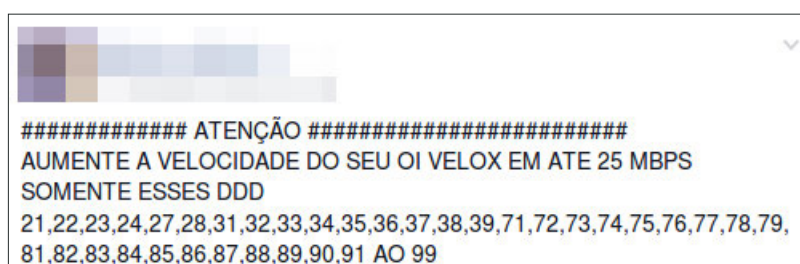


Figure 28: Post advertising Internet bump-up services

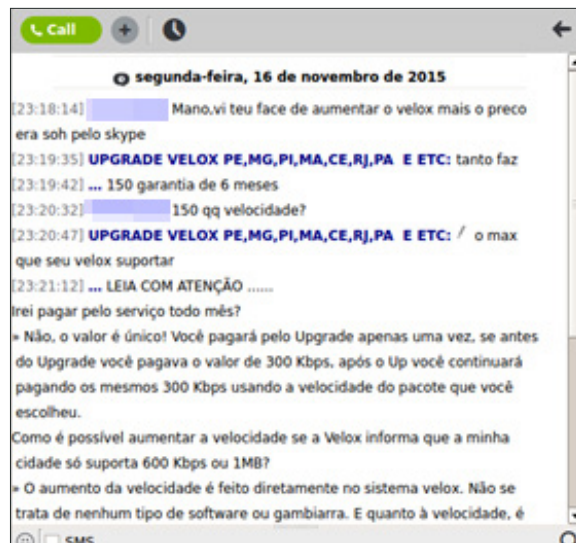


Figure 29: Conversation with a cybercriminal offering a bump-up service for Volex that costs R\$150 (US\$38.37) for a span of at least six months up to the maximum period that the provider supports

Crypters

Since many security vendors detect most known banking malware and other malicious files, crypters have become cybercrime staples. Most crypters are created via code splicing, entry point (EP) modification, executable binding, or general file modification. As in 2013, crypters can still be bought underground for R\$70 (US\$17.91). Some sellers even offer them at only R\$40 (US\$10.23) at year-end.

T.K CRYPTER PRIVADO

T.K É uma versão privada. Com o uso exclusivo você terá como segurar suas máquinas por mais de um mês sem que fique preocupado do projeto ficar detectado ou algo parecido.

Crypter 100% FUD = 60,00 Reais.

Promoção até o final de ano! = 40,00 Reais.

Conteúdo?

- + Recebe 2 Stubs. (100% FUD Ambas)
- + Client privado T.K!
- + Uso exclusivo.

Tempo de duração?

- + 30 Dias Premium.

Compatibilidade:

- + Sistemas operativos Windows.
- + Xp 32 e x64 Bits.
- + Windows XP Home e Professional. (SP1, SP2, SP3)
- + Windows Vista.
- + Windows 7.
- + Windows 8.

Figure 30: Post advertising a FUD crypter

A man in a dark suit is seen from the back and side, looking at a laptop screen. The background is a blurred office environment with other people and computer monitors. A large, semi-transparent circular graphic is overlaid on the image, containing the text.

SECTION 3

Challenges ahead

Challenges ahead

Brazil's socioeconomic landscape has made it the perfect breeding ground for cybercriminals. The quick returns promised by a life of cybercrime have made it enticing enough for several individuals to actually try it out. The tools and training they need are all out in the open. It only takes guts and know-how for any newbie to make it big. And given that cybercriminal activities are not as heavily penalized in Brazil as in other regions like North America, Brazilian cybercriminals publicly promote their operations. This, in turn, attracts more people to follow in their footsteps.

Although Brazilian cybercrime has continuously thrived on the Surface Web—again, mostly due to the cybercriminals' disregard for law enforcement—we foresee a big move to the Deep Web in the future. Developers and operators who use money mules and bank accounts to cash in their profits still have a high chance of getting caught. Using bitcoins and trading in darknets would decrease this risk.

Brazilian law enforcement agencies have an arduous task ahead if they ever want to topple local cybercrime. In 2015, we did see them exert more effort to fight cybercrime. Law enforcers partnered with security vendors like Trend Micro for cybercrime training and even collaborated in some investigations. These exercises were not enough to thwart cybercrime in Brazil though. Legislative bodies will have to be stricter with sanctions to discourage solo cybercriminal developers and operators. The national government needs to invest more resources for cybercriminal investigations, especially when Brazilian cybercrime moves into Deep Web territory. These tasks may be difficult now given the more pressing law enforcement challenges currently at play in the country.

We will continuously monitor Brazilian underground activities, trends, and offerings. Evidence of cryptocurrency adoption, especially now that ransomware—the very first local version—has emerged was observed. How this will change the current market dynamics, however, we have yet to find out.

References

1. Fernando Mercês. (2014). *Trend Micro Security Intelligence*. “The Brazilian Underground Market: The Market for Cybercriminal Wannabes?” Last accessed on 14 December 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf>.
2. Trend Micro. (30 June 2015). *TrendLabs Security Intelligence Blog*. “Lordfenix: 20-Year-Old Brazilian Makes Profit Off Banking Malware.” Last accessed on 15 December 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/lordfenix-20-year-old-brazilian-makes-profit-off-banking-malware/>.
3. Trend Micro Senior Threat Researchers. (13 April 2015). *Trend Micro Security Intelligence Blog*. “One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil.” Last accessed on 15 December 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/>.
4. Vanessa Martins. (27 August 2015). *globo.com*. “Police Arrest 20 Suspects to Clone Cards and Make Bank Fraud.” Last accessed on 15 December 2015, <http://g1.globo.com/goias/noticia/2015/08/policia-prende-20-suspeitos-de-clonar-cartoes-e-realizar-fraudes-bancarias.html>.
5. allpago. (2015). *allpago.com*. “The Spread of Internet Banking in LATAM.” Last accessed on 15 December 2015, <http://www.allpago.com/2015/08/the-spread-of-internet-banking-in-latam/>.
6. Trend Micro. (2015). *TrendLabs Security Intelligence Blog*. “Ransomware (Search Results).” Last accessed on 15 December 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence?s=ransomware>.
7. Sam S. Adkins. (May 2015). *Ambient Insight Research*. “The 2014–2019 Brazil Mobile Learning Market.” Last accessed on 15 December 2015, <http://www.ambientinsight.com/Resources/Documents/AmbientInsight-2014-2019-Brazil-Mobile-Learning-Market-Abstract.pdf>.
8. eMarketer Inc. (25 July 2014). *eMarketer*. “Brazil’s Bankers Get Digital, Both Online and via Mobile.” Last accessed on 15 December 2015, <http://www.emarketer.com/Article/Brazils-Bankers-Digital-Both-Online-via-Mobile/1011051>.
9. TrendLabs. (October 2015). *Trend Micro Security Intelligence*. “Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks.” Last accessed on 15 December 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-hazards-ahead.pdf>.
10. Fernando Mercês. (28 May 2015). *TrendLabs Security Intelligence Blog*. “DNS Changer Malware Sets Sights on Home Routers.” Last accessed on 16 December 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/dns-changer-malware-sets-sights-on-home-routers/>.
11. Lion Gu. (2015). *Trend Micro Security Intelligence*. “Prototype Nation: The Chinese Cybercriminal Underground in 2015.” Last accessed on 18 December 2015, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf>.
12. Trend Micro. (21 March 2014). *TrendLabs Security Intelligence Blog*. “Mass-Produced ATM Skimmers, Rogue PoS Terminals via 3D Printing?” Last accessed on 16 December 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/mass-produced-atm-skimmers-rogue-pos-terminals-via-3d-printing/>.

13. Trend Micro FTR Team. (April 2015). *Trend Micro Security Intelligence*. "FighterPOS: The Anatomy and Operation of a New One-Man PoS Malware Campaign." Last accessed on 16 December 2015, <https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/wp-fighterpos.pdf>.
14. Globo Comunicação e Participações SA. (16 November 2014). *globo.com*. "Gang Uses Bluetooth to Clone Chip Cards and Moves Millions." Last accessed on 18 December 2015, <http://g1.globo.com/fantastico/noticia/2014/11/quadrilha-usa-bluetooth-para-clonar-cartoes-de-chip-e-movimenta-milhoes.html>.
15. Brian Krebs. (27 October 2014). *Krebs on Security*. "'Replay' Attacks Spoof Chip Card Charges." Last accessed on 16 December 2015, <http://krebsonsecurity.com/2014/10/replay-attacks-spoof-chip-card-charges/>.
16. Trading Economics. (2015). *Trading Economics*. "Brazil Inflation Rate." Last accessed on 16 December 2015, <http://www.tradingeconomics.com/brazil/inflation-cpi>.
17. Cynthia Fujikawa Nes. (12 August 2015). *The Brazil Business*. "The Brazilian Educational System." Last accessed on 16 December 2015, <http://thebrazilbusiness.com/article/the-brazilian-educational-system>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud