A Trend Micro Research Paper

Brazil

Cybersecurity Challenges Faced by a Fast-Growing Market Economy

Trend Micro Incorporated

Contents

Introduction

This report presents an in-depth look at Brazil as part of our continuing research to understand the state of threats, cybersecurity, and the underground economy. This report can be viewed as a complement to "Latin American and Caribbean Cybersecurity Trends and Government Responses" published by the Organization of American States (OAS) and Trend Micro.[1]

Brazil is the largest country in the Latin American Region. This report shows that this bears out in the threats that Brazil faces, in some of the factors that drive these threats, and in the nature of the country's underground economy.

This report focuses on five areas of research:

1. Cybercrime trends
2. Reasons for increased cybercriminal activity
3. Brazil threats by the numbers
4. Underground activity
5. Cybersecurity public policy

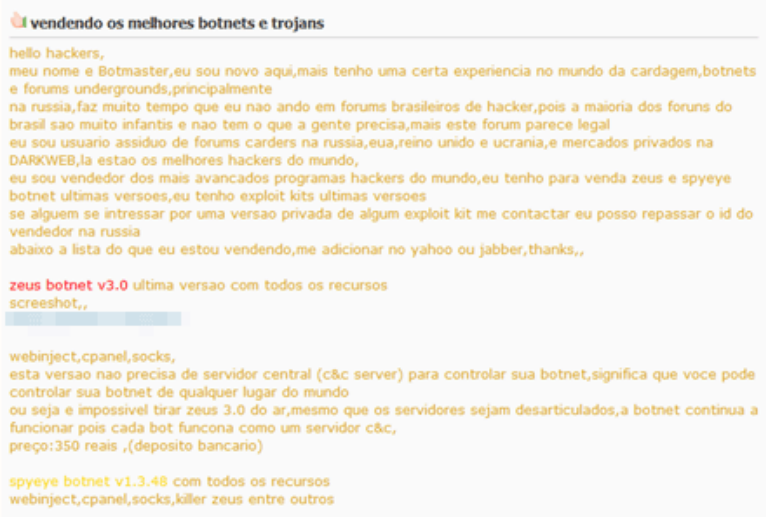
This report also aims to provide a broad but detailed view of the current state of cybersecurity in Brazil. As Brazil keeps pace with other so-called BRIC economies like Russia and China by having a vibrant and ever-expanding significance in the global economy, it is also experiencing the dark side of globalization. This is mainly due to the dramatic increase in cybercrime.

[1] Organization of American States and Trend Micro Incorporated. (2013). "Latin American and Caribbean Cybersecurity Trends and Government Responses." Last accessed July 30, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

Cybercrime Trends

Financial Crimes

Brazil is an economy on the move. The economic and geopolitical success of Brazil on the world stage is coupled by an ominous evolution of criminality. Brazil has become a significant source of numerous banking Trojans, which effectively exfiltrate sensitive financial data and credentials from corporate and personal computers (PCs). Perhaps the most famous is the BANCOS Trojan family, which is generally limited to gaining banking information within the Latin American Region. Recently, other banking Trojans like ZeuS, SpyEye, and CARBERP—all uncommon to the Brazilian threat landscape—have been found spreading in a myriad of Brazilian hacker forums.[2]


vendendo os melhores botnets e trojans

hello hackers,
meu nome e Botmaster,eu sou novo aqui,mais tenho uma certa experiencia no mundo da cardagem,botnets e forums undergrounds,principalmente
na russia,faz muito tempo que eu nao ando em forums brasileiros de hacker,pois a maioria dos foruns do brasil sao muito infantis e nao tem o que a gente precisa,mais este forum parece legal
eu sou usuario assiduo de forums carders na russia,eua,reino unido e ucrania,e mercados privados na DARKWEB,la estao os melhores hackers do mundo,
eu sou vendedor dos mais avancados programas hackers do mundo,eu tenho para venda zeus e spyeye botnet ultimas versoes,eu tenho exploit kits ultimas versoes
se alguem se intressar por uma versao privada de algum exploit kit me contactar eu posso repassar o id do vendedor na russia
abaixo a lista do que eu estou vendendo,me adicionar no yahoo ou jabber,thanks,,

zeus botnet v3.0 ultima versao com todos os recursos
screeshot,,

webinject,cpanel,socks,
esta versao nao precisa de servidor central (c&c server) para controlar sua botnet,significa que voce pode controlar sua botnet de qualquer lugar do mundo
ou seja e impossivel tirar zeus 3.0 do ar,mesmo que os servidores sejam desarticulados,a botnet continua a funcionar pois cada bot funcona como um servidor c&c,
preço:350 reais ,(deposito bancario)

spyeye botnet v1.3.48 com todos os recursos
webinject,cpanel,socks,killer zeus entre outros

Figure 1: Screenshot of an online ad selling known malware kits

The Brazilian Federation of Banks (FEBRABAN) reports that Brazilian bank fraud losses have decreased by 6.7% in 2012 compared with 2011. However, the US$1.4 billion lost in electronic fraud is still an attractive reason for cybercriminals to continue targeting the country's online banking users. This is especially true as the said amount represents only 0.06% of the money from total user transactions.[3] Note that 2013 ushered in a wave of successful heists and is on track to surpass the fraud losses in 2012.

[2] Ranieri Romera. (April 15, 2013). *TrendLabs Security Intelligence Blog.* "New Crimeware in BANCOS Paradise." Last accessed June 24, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/new-crimeware-in-bancos-paradise/.

[3] Brazilian Federation of Banks. (December 2012). *CIAB Febraban.* "Tecnologia para Acelerar." Last accessed June 25, 2013, http://www.ciab.com.br/_pdfs/publicacoes/2012/43-Dez2012.pdf.

Reasons for Increased Cybercriminal Activity

Large Online Population

With over 201 million inhabitants, Brazil ranks as the most populated country in Latin America and fifth in the world.[4] Brazil's huge population contributes to its large share of Internet users at almost 88.5 million.[5]

As of 2011, nearly two in five Brazilian (38%) households already had Internet access.[6] Due to sheer population size, Brazil has become a magnet for cybercriminals who see online users as a lucrative market for illegal activity.

Robust Internet Connectivity

The average connection speed in Brazil continues to increase. Over a tenth (13%) of the Internet users in the country now enjoys Internet speeds of above 4Mbps.[7] As such, Internet access has become a popular commodity in Brazil. Consumers spend over 27 hours per month on their computers—the highest average engagement in Latin America.[8]

Brazil's progression toward a connected society also serves as a catalyst for sophisticated cybercriminal activities.

---

4 Central Intelligence Agency. (June 12, 2013). *CIA—The World Factbook.* "Country Comparison: Population." Last accessed June 20, 2013, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html?countryName=Brazil&countryCode=br&regionCode=soa&rank=5#br.

5 Miniwatts Marketing Group. November 27, 2012. Internet World Stats. "Brazil Internet Stats and Telecom Market Report." Last accessed, June 20, 2013, www.internetworldstats.com/sa/br.htm.

6 Organization of American States. (June 21, 2012). *OAS Cyber Security Program.* "Overview of Information Security (Cyber Security and Cyber Defense of Critical Infrastructure in Brazil)." Last accessed June 20, 2013, http://www.oas.org/cyber/presentations/OAS%20set%202012.pdf.

7 Akamai. (April 22, 2013). "The State of the Internet 4th Quarter 2012 Report." Last accessed June 20, 2013, http://www.akamai.com/dl/whitepapers/akamai_soti_q412.pdf?curl=/dl/whitepapers/akamai_soti_q412.pdf&solcheck=1&WT.mc_id=soti_Q412&.

8 comScore, Inc. (March 2013). "2013 Brazil Digital Future in Focus." Last accessed June 20, 2013, http://www2.comscore.com/l/1552/ure-in-Focus-Final-English-pdf/3cyltr.

Active Online Banking Community

Brazil has become the forefront of online banking due to its economic history. From the 1980s to the early 1990s, Brazil's hyperinflation pushed its government and financial systems to drastically adapt to stabilize the economy.[9]

To accomplish this, Brazilian banking institutions pioneered electronic and online banking systems, tossing over check-clearing systems, thus making way to more rapid money movement.

Today, we see a very robust online banking community as well as widespread Internet connectivity in Brazil due to early efforts to embrace the Internet and online banking.

ICT Development

Brazil is the world's eighth-largest economy based on gross domestic product (GDP) by purchasing power parity (US$2.394 trillion). As with other top and emerging markets, the country is experiencing notable growth in the information and communication technology (ICT) market.

Brazil also has the third-largest computer market, fourth-largest cellular phone and automotive markets, second-largest automated teller machine (ATM) market, and fifth-largest medical equipment market.

The OAS predicts that the ICT market revenue in Brazil will reach between US$150 and US$200 billion by 2020 from US$102 billion in 2011.

In 2012, Brazil ranked highly in the Latin American and Caribbean Region in terms of most number of Internet-facing industrial control systems (ICS).

[9] James Dale Davidson. (2012). *Google Books.* "Brazil Is the New America: How Brazil Offers Upward Mobility in a Collapsing World." Last accessed July 15, 2013, http://books.google.com.ph/books?id=8muXHC8xQBIC&pg=PT125&img=1&zoom=3&hl=en&ots=yf3cfKKtQR&sig=ACfU3U1214BNCrmKbjl6ora5b4ccYOF1Ow&w=685.

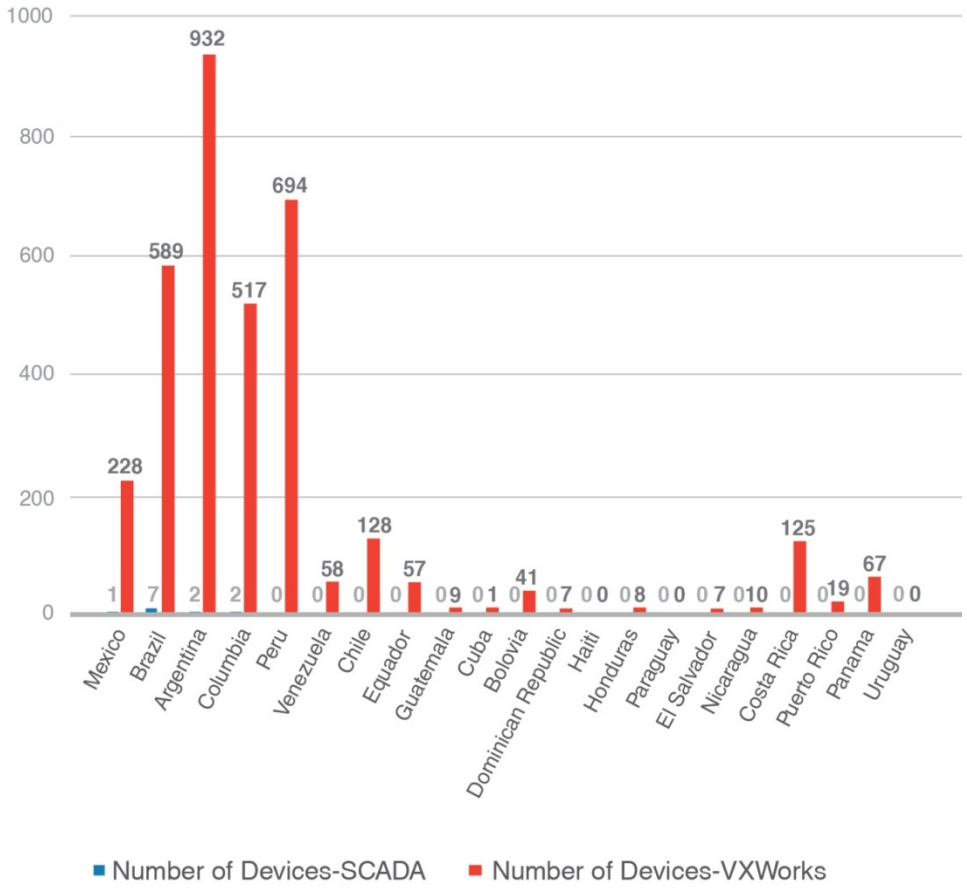


Figure 2: Number of Internet-facing SCADA and VxWorks Devices in the Latin American and Caribbean Region

Increased emphasis on the ICT market led to growth in investments in the research and development (R&D) sector. The dependence on ICT infrastructure then rose among various sectors of the Brazilian society.

The breadth of information that follows ICT development is a beacon for cybercriminals with malicious intent, ranging from crippling critical infrastructure to stealing sensitive data. Attacks on ICS should not be viewed as sole attempts to steal sensitive data from the energy or government sectors. Political and social unrest via nonstate actors are being expressed via purposeful hacking and defacement. Public discontent will usher in localized attacks as a form of public expression in 2013.

Lax Legal Measures

The 2013 BSA Global Cloud Computing scorecard recognized Brazil's cybersecurity efforts with the passing of modern cybercrime legislations. However, the report revealed that some major cloud security measures remain incomplete.[10]

Data privacy per personal information remains an issue as the *Data Protection Bill* still awaits approval. This bill promises general data protection coverage, which includes requiring companies to notify customers and partners in case of a breach.

The report said that, apart from computer-related crimes, the bills passed in 2012 were vague, making it harder to arrest a hacker if he/she commits a cybercrime. Since the actual bills are vague, it is necessary to judge some cybercrimes with traditional laws and try to adopt traditional laws to interpret those cybercrimes when there is no clear evidence of financial theft. This kind of situation can leave room for interpretation and some inefficiency to accuse cybercriminals.[11]

Brazil has also yet to sign the *World Intellectual Property (WIPO) Copyright Treaty,* which seeks to protect authors' rights to their literary and artistic works.[12]

Lack of Cybersecurity Training

Based on a survey on cybercrime in 2011, more than half (57%) of the total number of organizations in Brazil do not have the capacity or know if they are capable of investigating cybercrime. Exactly half (50%) were equally unaware if their organizations could detect and prevent cybercrime.[13] Another two out of five Brazilians surveyed by PricewaterhouseCoopers (PwC) also said they have not received cybersecurity training in 2011.

---

10 BSA: The Software Alliance. (March 2013). "2013 BSA Global Cloud Computing Scorecard Country: Brazil." Last accessed June 20, 2013, http://cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_Brazil.pdf.

11 Tony Smith. (October 27, 2003). *The New York Times.* "Technology: Brazil Becomes a Cybercrime Lab." Last accessed July 9, 2013, http://www.nytimes.com/2003/10/27/business/technology-brazil-becomes-a-cybercrime-lab.html?src=pm.

12 World Intellectual Property Organization. (December 20, 1996). "WIPO Copyright Treaty." Last accessed June 23, 2013, http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html.

13 PricewaterhouseCoopers LLP. (2011). "Cybercrime Protecting Against the Growing Threat, Global Economic Survey 2011." Last accessed June 20, 2013, http://www.pwc.com.br/pt/publicacoes/assets/pesquisa-crimes-digitais-11-ingles.pdf.

Brazil Threats by the Numbers

Malware

DOWNAD, more widely known as "Conficker," dominated Brazil's malware count. Along with the substantial presence of key generators, cracks, hacking tools, and autorun malware, DOWNAD shows that the majority of the country's Internet users still resort to pirated software use for their computing needs. This is because pirated software cannot be updated with the latest patches, leaving them exposed to malware like Conficker. The prevalence of DOWNAD also reveals a cultural indifference as well as difficulty with enterprise policies and processes toward regularly patching systems that could help prevent infection with the said malware.

The DORKBOT worm also continued to plague Internet users in Brazil since it first became prominent in the Latin American Region in 2011. This worm spreads across Internet Relay Chat (IRC) bots to perform distributed denial-of-service (DDoS) attacks. DORKBOT is most notable for its ability to steal user credentials by monitoring website forms. It also tries to use nicknames to pinpoint user locations, which are then used to coordinate effective DDoS attacks.[14]

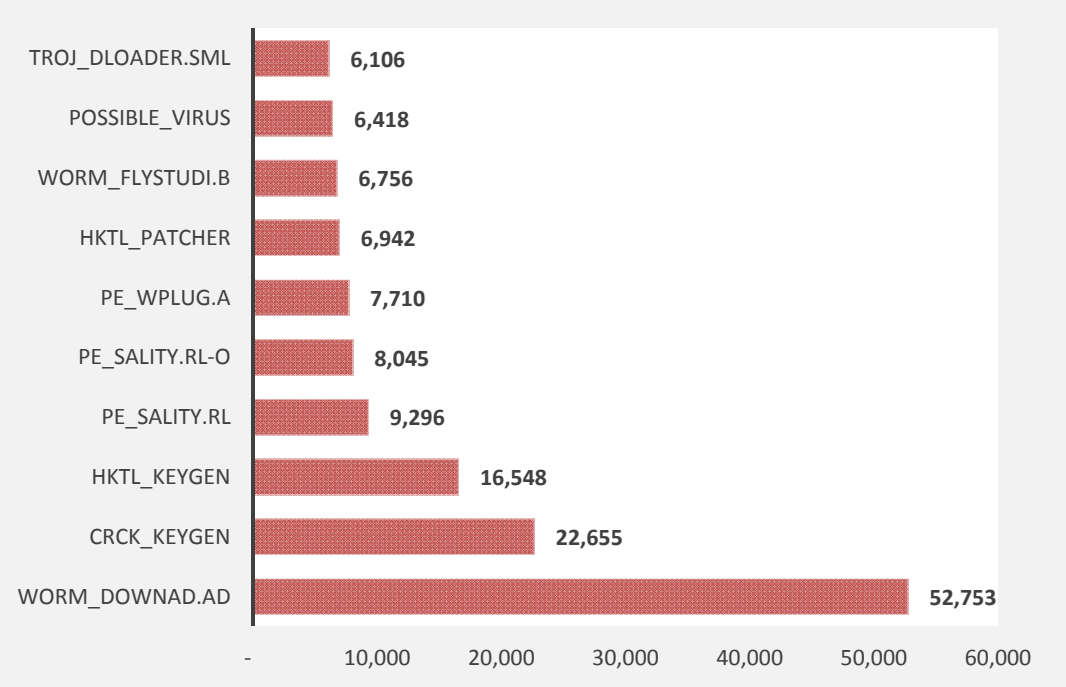


Figure 3: Top 10 malware in Brazil, 1Q 2012–1Q 2013

[14] Trend Micro Incorporated. (2013). *Threat Encyclopedia.* "WORM_DORKBOT: IRC Bots Rise Again?" Last accessed June 23, 2013, http://about-threats.trendmicro.com/us/webattack/102/wormdorkbot%20irc%20bots%20rise%20again.

Spam

Brazil sends out the most number of spam in Latin America. Almost two out of five (38%) malicious emails from the region comes from Brazil. This can be explained by the relatively high population count and unpatched systems turned into botnets for spamming. Lack of education on the dangers of phishing and spamming also runs rampant, making Internet users more vulnerable to social engineering scams and other email-based attacks.

Figure 4: Latin American spam-sending country share breakdown

	Country Name	Volume Share
1	Brazil	36.30%
2	Mexico	18.10%
3	Argentina	11.90%
4	Colombia	9.10%
5	Chile	5.54%
6	Peru	4.70%
7	Venezuela	3.62%

	Country Name	Volume Share
8	Costa Rica	1.30%
9	Uruguay	1.20%
10	Ecuador	1.19%
11	Panama	1.16%
12	Dominican Republic	1.06%
13	Puerto Rico	0.83%
14	Guatemala	0.51%
15	Bolivia	0.50%
16	El Salvador	0.36%
17	Paraguay	0.36%
18	Nicaragua	0.30%
19	Trinidad and Tobago	0.30%
20	Honduras	0.24%
21	Jamaica	0.22%
22	Haiti	0.22%
23	Bahamas	0.18%
24	U.S Virgin Islands	0.14%
25	Belize	0.11%
26	Guadeloupe	0.08%
27	Antigua and Barbuda	0.07%
28	Martinique	0.06%
29	Barbados	0.06%
30	Cuba	0.05%
31	Cayman Islands	0.05%
32	Aruba	0.04%
33	French Guiana	0.02%
34	Guyana	0.02%
35	Saint Lucia	0.02%
36	Suriname	0.02%

	Country Name	Volume Share
37	Grenada	0.02%
38	Saint Vincent and the Grenadines	0.02%
39	Saint Kitts and Nevis	0.01%
40	British Virgin Islands	0.01%
41	Dominica	0.01%
42	Turks and Caicos Islands	0.00%
	Total	**100.00%**

Table 1: Ranking of Latin American countries based on the volume of spam sent out

Malicious URLs

The majority (58%) of malicious URLs in the Latin American Region were hosted in Brazil. Malicious URLs and attacks that compromise legitimate sites are flourishing in the region. Hackers prefer this tactic, as it has been proven to bypass traditional perimeter defenses.

Figure 5: Latin American malicious-URL-hosting country share breakdown

	Country Name	Volume Share
1	Brazil	58.04%
2	Mexico	12.35%
3	Argentina	8.66%
4	Chile	6.17%
5	Colombia	4.85%
6	Panama	1.85%
7	Venezuela	1.68%
8	Dominican Republic	1.36%
9	Puerto Rico	0.99%
10	Peru	0.80%
11	Costa Rica	0.55%
12	Bolivia	0.54%
13	Ecuador	0.50%
14	Guadeloupe	0.20%
15	British Virgin Islands.	0.20%
16	Guatemala	0.15%
17	Bahamas	0.15%
18	El Salvador	0.12%
19	Jamaica	0.11%
20	Uruguay	0.09%
21	Trinidad and Tobago	0.09%
22	Honduras	0.09%
23	French Guiana	0.06%
24	Barbados	0.06%
25	Haiti	0.04%
26	Nicaragua	0.04%
27	Martinique	0.04%
28	St. Lucia	0.04%
29	U.S. Virgin Islands	0.03%
30	Paraguay	0.03%
31	Cayman Islands	0.02%
32	Belize	0.02%
33	Dominica	0.01%
34	Saint Kitts and Nevis	0.01%

	Country Name	Volume Share
35	Antigua and Barbuda	0.01%
36	Turks and Caicos Islands	0.01%
37	Grenada	0.01%
38	Saint Vincent and The Grenadines	0.01%
39	Guyana	0.01%
40	Aruba	0.01%
41	Cuba	0.00%
	Total	**100.00%**

Table 2: Ranking of Latin American countries that host malicious URLs

Botnets

Brazil is known as an active ground for command-and-control (C&C) servers and compromised computers that take part in large data-stealing botnet operations.

Botnets are composed of numerous infected computers, which cybercriminals can use to send out spam and perform other illegal online activities. The bigger the botnet, the more powerful it is. Brazil has relatively large numbers of C&C servers and connections worldwide.

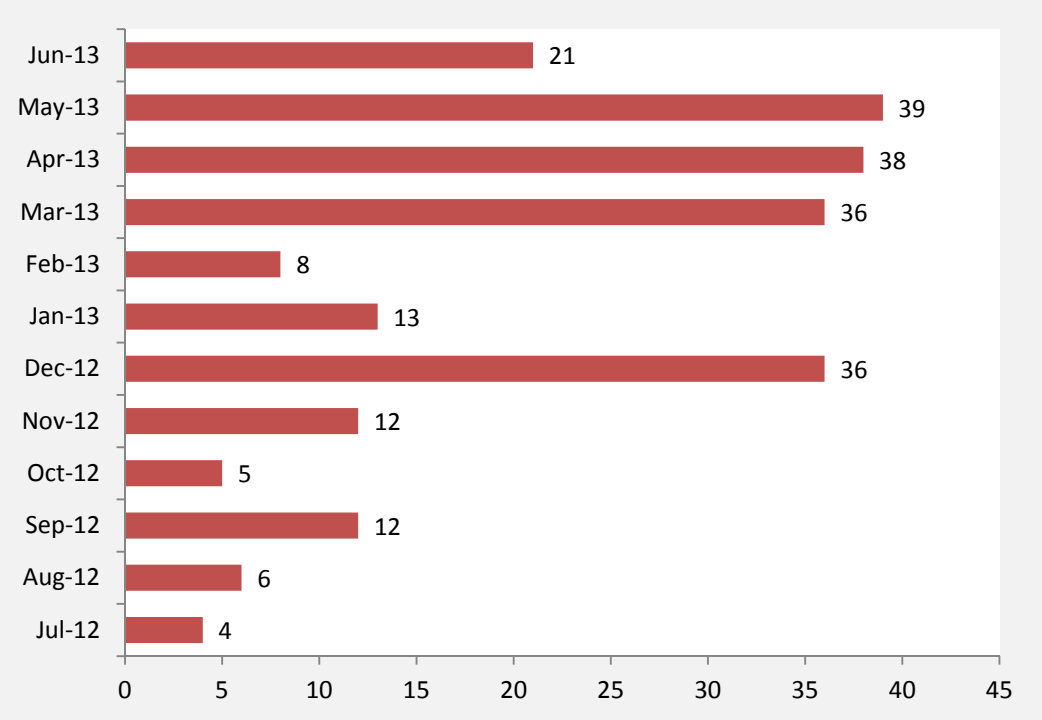


Figure 6: Number of botnet C&C servers detected per month, July 2012–June 2013

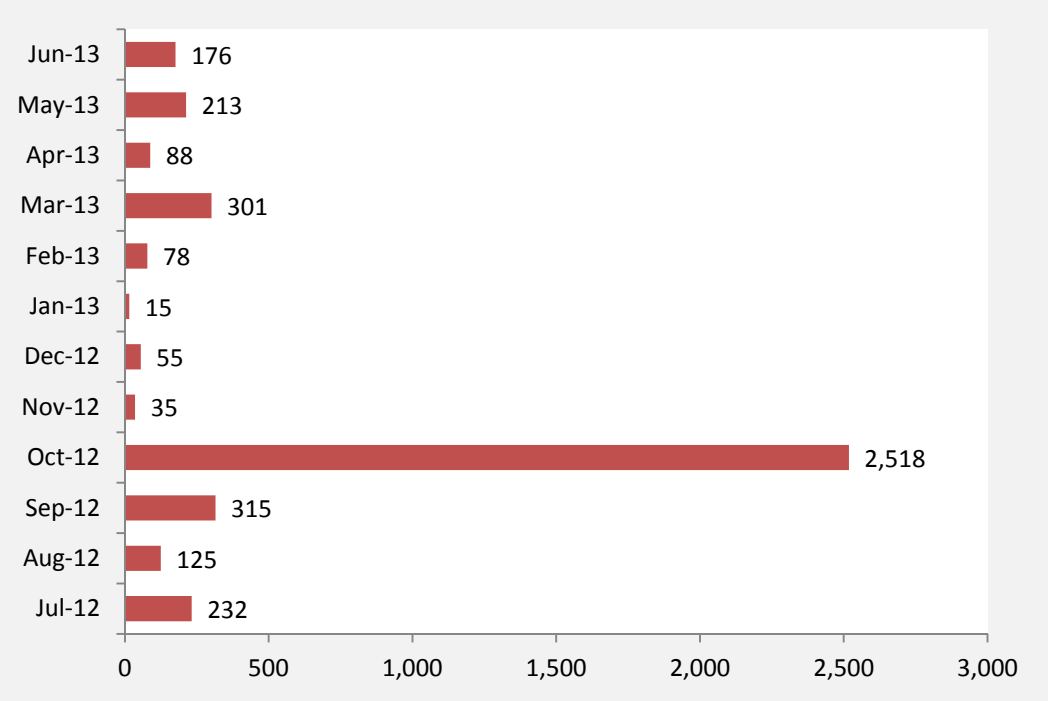


Figure 7: Number of botnet C&C connections detected per month, July 2012–June 2013

Mobile

Almost nine in 10 (86%) consumers in Brazil use mobile phones and almost four in 10 (36%) use smartphones. The sheer size of the mobile market and the popularity of activities like mobile banking and shopping in the country make it a lucrative target for phishing scams and mobile malware threats.[15]

[15] Nielsen. (February 2013). "Mobile Consumer Report 2013." Last accessed, August 20, 2013, www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2013%20Reports/Mobile-Consumer-Report-2013.pdf.

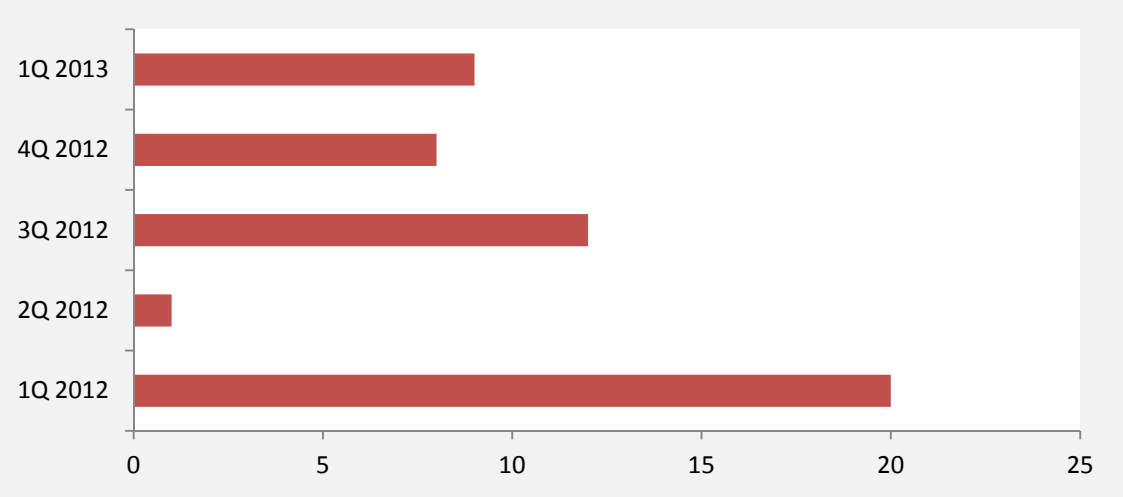


Figure 8: Mobile financial phishing site volume, 1Q 2012–1Q 2013

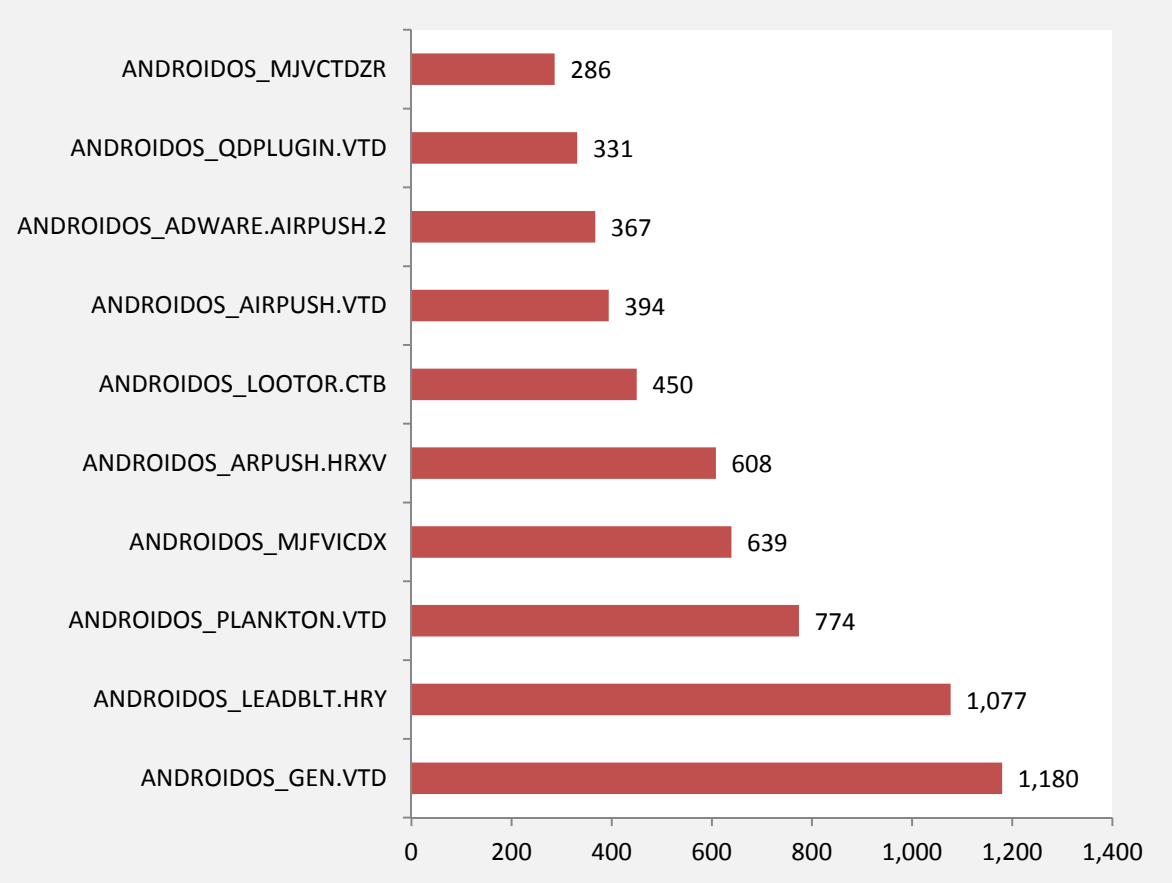


Figure 9: Top 10 Android malware families, 1Q 2012–1Q 2013

	Country Name	Volume Share
1	Serbia	15.85%

2	Chile	6.78%
3	India	6.25%
4	Philippines	6.19%
5	Belgium	5.93%
6	**Brazil**	**5.57%**
7	Bulgaria	5.56%
8	Nepal	5.26%
9	Tunisia	5.17%
10	South Korea	4.74%

Table 3: Brazil's ranking among countries most at risk of privacy exposure due to app use, 1Q 2012–1Q 2013

	Country Name	Volume Share
1	Iran	15.26%
2	Nigeria	14.10%
3	Nepal	12.29%
4	Belarus	10.67%
5	Chile	10.17%
6	Kuwait	7.77%
7	India	7.07%
8	Tunisia	5.17%
9	Russia	5.16%
10	Philippines	4.59%
11	Vietnam	4.35%
12	Ukraine	4.03%
13	Italy	4.02%
14	**Brazil**	**3.90%**
15	Turkey	3.71%

Table 4: Brazil's ranking in terms of malicious Android app download volume, 1Q 2012–1Q 2013

	Country Name	Volume Share
1	Canada	33.33%
2	Ireland	32.41%
3	Japan	30.62%
4	Philippines	26.15%
5	China	25.31%
6	Netherlands	24.26%
7	Puerto Rico	23.08%
8	United States	23.08%
9	Indonesia	21.43%
10	Russia	20.86%
11	Germany	20.78%
12	South Korea	20.55%
13	Singapore	19.09%
14	Malaysia	18.66%
15	Australia	17.75%

	Country Name	Volume Share
16	Saudi Arabia	17.59%
17	Turkey	16.06%
18	Nigeria	16.00%
19	India	15.96%
20	Spain	15.79%
21	Italy	14.77%
22	Mexico	14.28%
23	Hong Kong	13.83%
24	France	13.75%
25	Thailand	13.34%
26	Taiwan	12.90%
27	Israel	12.50%
28	United Kingdom	12.48%
29	Slovakia	11.36%
30	Iraq	10.64%
31	Costa Rica	10.20%
32	**Brazil**	**10.13%**
33	Denmark	10.00%
34	United Arab Emirates	8.96%
35	Poland	8.07%

Table 5: Brazil's ranking in terms of battery-draining app download volume, 1Q 2012–1Q 2013

Underground Activity

Online Banking Theft

Over 50% of Brazilians use e-finance services—electronic means of communication and computation for financial services—causing them to be targeted by organized crime groups using tailor-made BANCOS malware.[16]

Brazil is known for the wide use of BANCOS malware in online banking theft. BANCOS comprises spyware and Trojan malware, which steal online banking credentials by displaying spoofed pages and logging keystrokes.

[16] Franklin Allen, James McAndrews, and Philip Strahan. (October 7, 2001). "E-Finance: An Introduction." Last accessed July 9, 2013, http://fic.wharton.upenn.edu/fic/papers/01/0136.pdf.

Other malware strains also plague the Brazilian threat landscape. In TSPY_BANDOC.A's case, the target is not to steal bank information as BANCOS malware usually do. Since March 2013, BANDOC has started wreaking havoc among the users of Boleto Bancário, an online payment system for transferring money among individuals, companies, and other groups.[17] This malware family can change the boleto (or "ticket") document whenever users generate them on e-commerce or online banking sites. The figure shown below highlights the barcode and numeric code, which the malware alters.

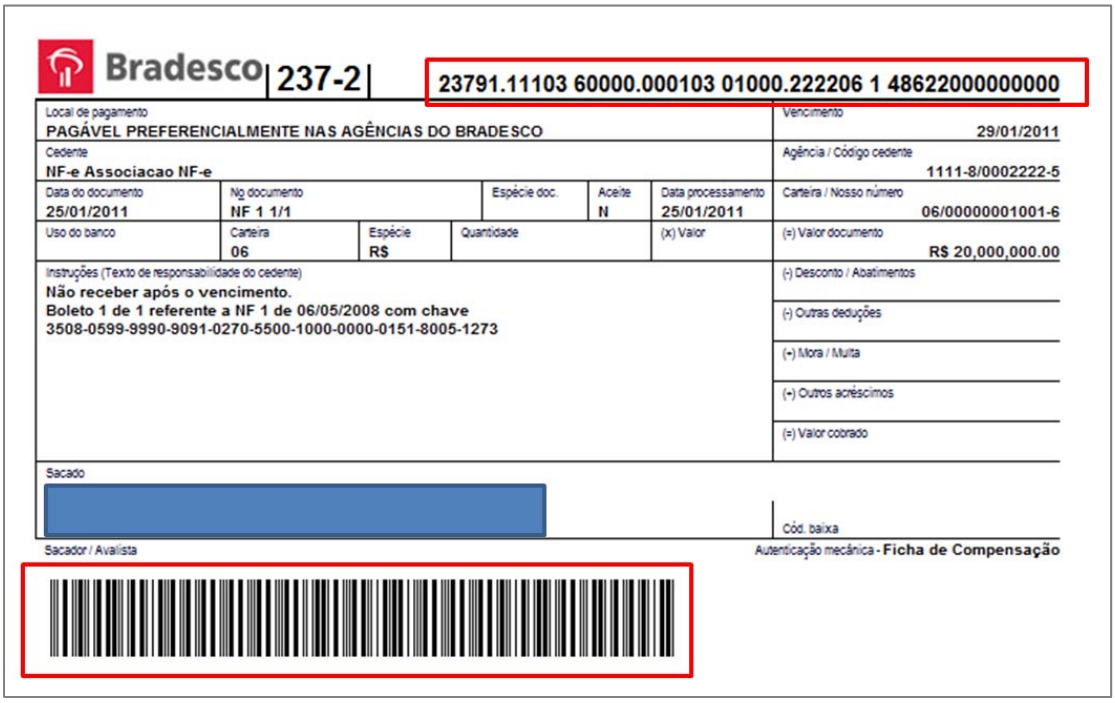


Figure 10: Sample boleto used for financial transactions in Brazil

BANDOC malware force users to type the numeric code above by inserting additional bank spaces into the bar code. It then changes the first part of the numeric code to route the money to another account while retaining the last part of the code to preserve the expiration date and value.

[17] ABOUT-PAYMENTS.com. (July 9, 2013). "Boleto Bancário Pay." Last accessed July 9, 2013, http://www.about-payments.com/payment-methods/boleto-bancario-pay.

Similarly, variants of the data-stealing BANKER malware thrive in the Brazilian threat landscape. BANKER strains often steal banking credentials and email account details through phishing pages that mimic official banking sites. Stolen information is then sent to predetermined email addresses, drop zones in hosted servers, or URLs via HTTP POST.[18]

Figure 11: Screenshots of Orkut phishing mail that lead to the download of TROJ_BANKER

[18] Trend Micro Incorporated. (June 26, 2013). *Threat Encyclopedia.* "BANKER." Last accessed June 26, 2013, http://about-threats.trendmicro.com/us/malware/banker.

At the "World Economic Forum Financial Sector Security Summit" held in Washington D.C. on June 2013, it was noted by the major Brazilian financial institutions that the number of online fraud incidents has dramatically increased in the first half of 2013. Cybercriminals are also finding innovative ways to deliver online banking malware and steal banking credentials in Brazil. Man-in-the-browser (MiTB) attacks are being used to bypass the Adobe® Flash® Player plug-in security system that the financial institutions deployed to combat keystroke loggers.

In addition, crafty cybercriminals also utilize watering hole attacks to target individuals. Recently compromised Brazilian government sites and browsers were used to directly install malware or lure users into providing sensitive information.[19] These types of attack are flourishing, as the Brazilian hacker has become appreciative of this tactic.

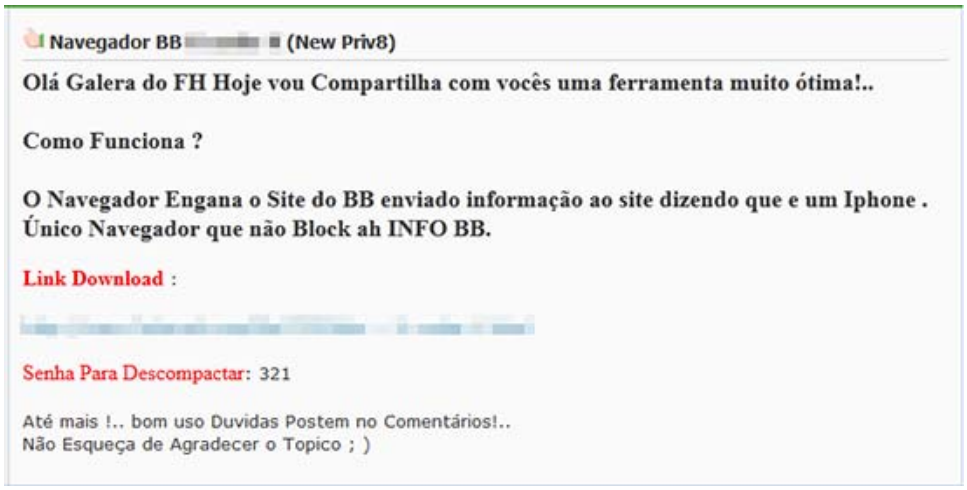


Figure 12: Screenshot of forum post offering a browser for the Banco do Brasil site

[19] Roddell Santos. (May 28, 2013). *TrendLabs Security Intelligence Blog.* "BANKER Malware Hosted in Compromised Brazilian Government Sites." Last accessed June 24 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/banker-malware-hosted-in-compromised-brazilian-government-sites/; Ranieri Romera. (May 7, 2013). *TrendLabs Security Intelligence Blog.* "Homemade Browser Targeting 'Banco do Brasil' Users." Last accessed June 24, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/homemade-browser-targeting-banco-do-brasil-users.

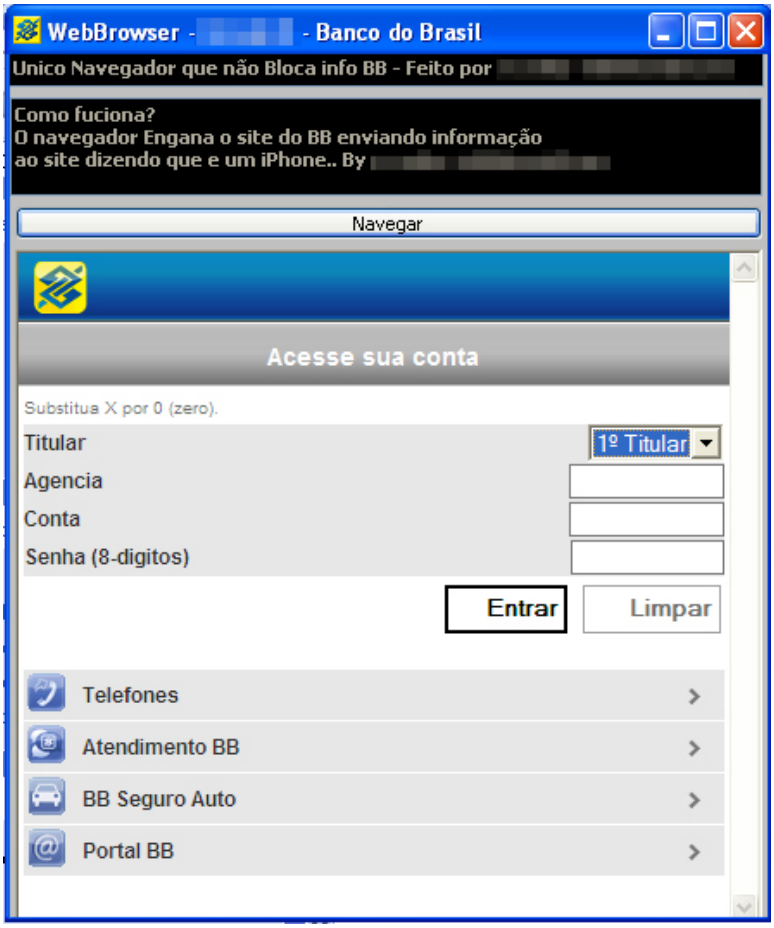


Figure 13: Screenshot of homemade browser used to lure users to reveal information

Cybercriminal Underground

The cybercriminal underground economy of Brazil mimics that of most countries in the Latin American Region. As with others, cybercriminals in Brazil exchange wares on hacker forums and popular social networking sites.

Figure 14: Screenshot of ads selling stolen information on Orkut

Cybercriminals in Brazil distribute source code for malware, also like in other countries in the Latin American Region. The only difference is, instead of popular crimeware kits like ZeuS, locals prefer to buy the BANCOS source code.

The Brazilian underground economy is also filled with exchanges for credit card information, personally identifiable information (PII), bank account information, virtual private server (VPS) hosting services, phishing kits, email spam distribution lists, mail listings, and others. These items are usually hosted in one of the following services:

- 000webhost
- Byet Host
- AwardSpace
- P4O
- Zymic
- x10Hosting
- Xp3
- my3GC

Cybercriminals in Brazil also perform monetary exchanges for hacker training, forming cybercriminal schools on demand. They prefer direct money transfers using mules' accounts as payment method when selling underground services or products.

Notably, the Brazilian cybercriminal underground stands out with its hackers' collaborative drive that is starting to show in the threats produced in the region.

One such product is Picebot, a US$140 sophisticated crimeware kit using new malicious code. Picebot shows that cross-regional underground activities actively happen between hackers in Brazil. It also shows that, like other countries in the region, the Brazilian cybercriminal underground is on its way to become a more structured ecosystem where hackers are assigned their own roles, either as developers or sellers.

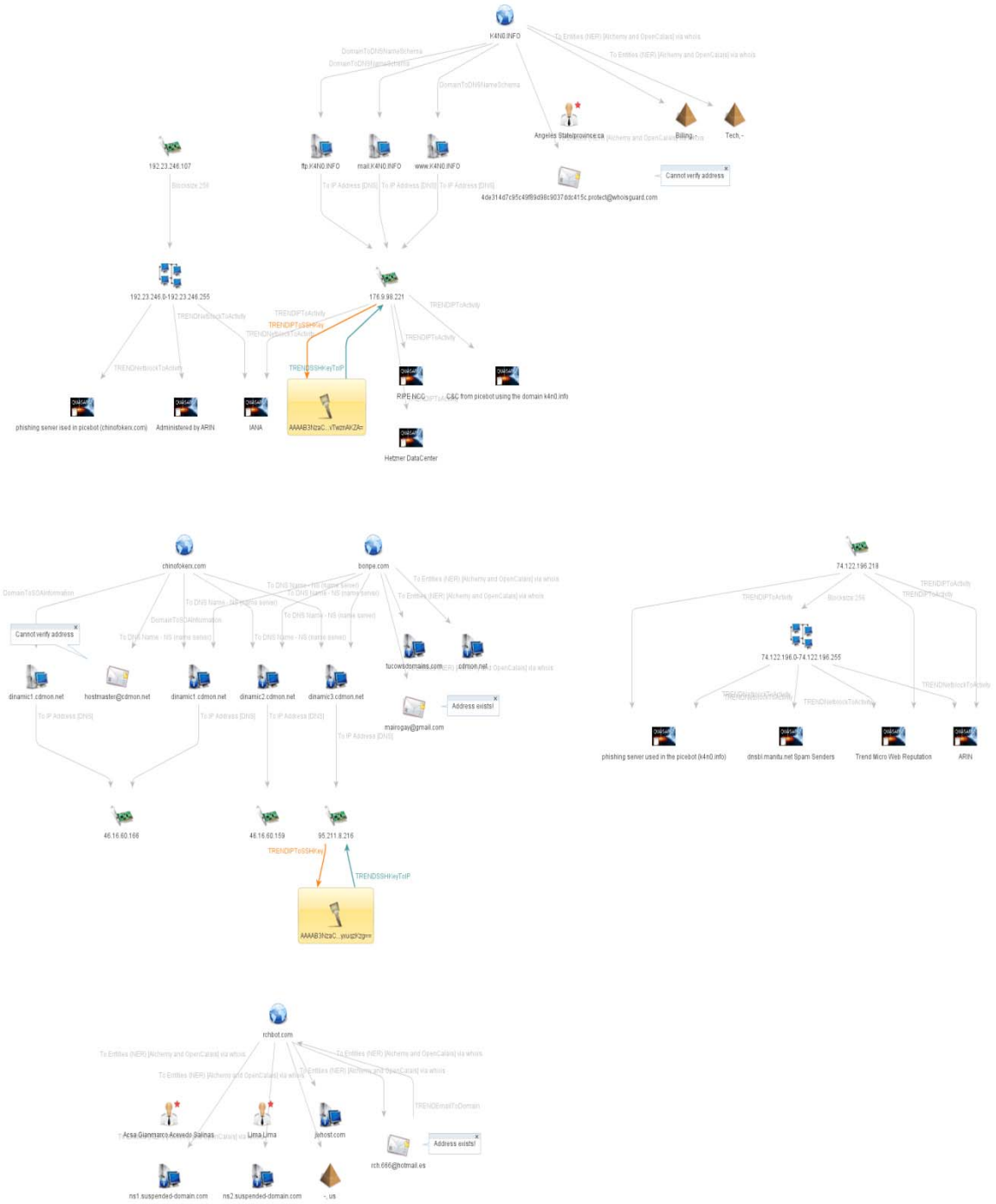


Figure 15: Picebot's botnet structure

Cybercriminal Underground Price List

Product	Price (Brazilian Real)	Price (U.S.$)
Credit card information	R$700 for information from 10 credit cards	US$312.82 for information from 10 credit cards
Credit card info-stealing kit	R$5,000	US$2,234.43
Crypter	R$100 for 30 days	US$44.69 for 30 days
Domain Name System (DNS) pharming	R$5,000	US$2,234.43
Hosting	R$50	US$22.34
Malicious Java applet	R$80	US$35.75
Facebook malware	R$70	US$31.28
VPS for spam	R$70	US$31.28
Credit card checker	R$400	US$178.75
Coding service	R$500	US$223.44

Table 6: Prices across the Brazilian cybercriminal underground

Hacktivism

These days, hacktivism is growing at an exponential rate in Brazil.

Figure 16: Screenshot of a hacktivist group announcement of government site takedowns

Hacktivists in Brazil may not be as organized as those in other countries but we predict that it is only a matter of time before this form of protest becomes more structured and popular in the country.

Conclusion

Brazil, as an economy, is growing and taking its place on the world stage, and criminals are aware of this. The traditional criminal syndicates have adopted the methods of cybercriminals. The country has experienced unique problems with banking Trojans for years. As Brazil grows and evolves, the unique homegrown problems it faces will grow as well. A rising economic tide lifts all boats and that includes those of cybercriminals.

This economic growth fosters cyber externalities as those who enjoy high-speed connectivity are not being targeted by sophisticated cybercriminals. Brazil is seeing some of the fastest growth in terms of new Internet users worldwide. Unfortunately, this means Brazil also has one of the largest potential pools of uneducated and unsophisticated users for cybercriminals to target. Lack of broad, basic end-user education means that attackers and criminals are able to successfully target users with unsophisticated attacks that may not succeed in other countries. This reality sheds light on why Brazil is the leading source of spam in Latin America.

Research shows that Conficker's major presence in Brazil underscores concerns surrounding users who have not been taught critical basic cybersecurity practices. Patches that can protect systems from Conficker and signatures that can protect and remove the malware have been available for over four years now. That Conficker remains an issue indicates a widespread failure to follow best practices on software patching, including running security software and updating it.

Finally, we see that Brazil's unique social, linguistic, and cultural heritage within the Latin America Region is reflected in its criminal underground through one of the most basic expressions of culture on the Internet—social networking sites. Unique to the Latin American Region, Brazilian cybercriminals rely on Orkut as their preferred forum for interaction and exchange.

While the state of threats and the underground economy is expansive in Brazil, like other countries in the Latin American Region, the government and law enforcement agencies are working to play catch up to some degree. While there has been good motion forward in the area of legislation, it is clear that more is needed in terms of recruitment and training cybersecurity specialists in law enforcement and laws that can support their pursuit and conviction of cybercriminals.

As we broadly saw within the Latin American Region in "Latin American and Caribbean Cybersecurity Trends and Government Responses," successfully meeting the challenges in Brazil requires political will, law enforcement resources, and a robust, ongoing public-private partnership (PPP) with Internet service providers (ISPs), security companies, and hardware and software vendors.

Appendix

Cybersecurity Public Policy

Cybercrime Laws

1. **2008 National Strategy of Defense:** Strengthened Brazil's military network infrastructure and led to the creation of Brazil's Center for Cyber Defense for the protection of its public administration networks.[20]

2. **Azeredo Law:** Named after then-Senator Eduardo Azeredo who proposed the bill in 2008, it is the revised version of *Proposed Law (PL) 84/99,* also known as the *"Digital Crimes Bill"* or the *"Brazilian Cybercrime Bill,"* which was critiqued for using vague language that would have criminalized ordinary Internet activities if passed.[21]

   The *Azeredo Law* excluded 17 controversial articles from the original proposal and only retained provisions to create a police structure against cybercrime, and battle racism, treason, and the falsification of private document or electronic data.[22]

3. **Carolina Dieckmann Law (PL 2793/11):** This law was named in reference to the actress whose intimate photos were released online. It criminalizes unauthorized access and theft of emails and other online sources of sensitive information.[23]

---

20 James Lewis and Katrina Tamlin. (2011). "Cybersecurity and Cyberwarfare 2011." Last accessed June 24, 2013, http://web.archive.org/web/20120131124638/http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

21 Paula Góes. (July 17, 2008). *Global Voices Online.* "Brazil: Bloggers Question the 13 New Cybercrimes." Last accessed June 24, 2013, http://globalvoicesonline.org/2008/07/17/brazil-bloggers-question-the-13-new-cyber-crimes; Center for Democracy and Technology. (November 7, 2011). "Comments on Brazil's Proposed Law 84/99." Last accessed June 24, 2013, https://www.cdt.org/files/pdfs/CDT-Brazil_PL84-99_comments-2011.pdf.

22 Felipe Ventura. (November 3, 2012). "Dieckmann x Azeredo: Como se Comparam os Dois Projetos de lei para Crimes Virtuais." Last accessed June 24, 2013, http://gizmodo.uol.com.br/projeto-leis-dieckmann-azeredo/.

23 *Universo Online.* (July 11, 2012). "Câmara Aprova lei Que Criminaliza Invasão de E-mail e Fraude de Cartões via Internet." Last accessed June 24, 2013, http://tecnologia.uol.com.br/noticias/redacao/2012/11/07/camara-aprova-tipificacao-de-crimes-praticados-com-uso-da-internet.htm.

Government Bodies

1. **Gabinete de Segurança Institucional (GSI)/Institutional Security Cabinet:** This is an executive cabinet office that deals with national ICT security issues as well as crisis management and intelligence for military and security issues.[24]

2. **Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR-GOV)/Treatment Center Security Incident of Computer Networks Federal Public Administration:** This agency is tasked to investigate security incidents in computer networks that involve the Brazilian federal government.[25]

3. **Comitê Gestor de Segurança da Informação (CGSI)/Steering Committee for Information Security:** The CGSI was created by Decree No. 3505 of June 13, 2000. It is an information security steering committee that advises the Executive Secretariat of the National Defense Council, defines cybersecurity policy direction, and evaluates and examines information security issues.[26]

4. **Computer Emergency Response Team Brazil (CERT.br):** This is the Brazilian Computer Emergency Response Team, sponsored by the Brazilian Internet Steering Committee. Its assignments include receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet.[27]

---

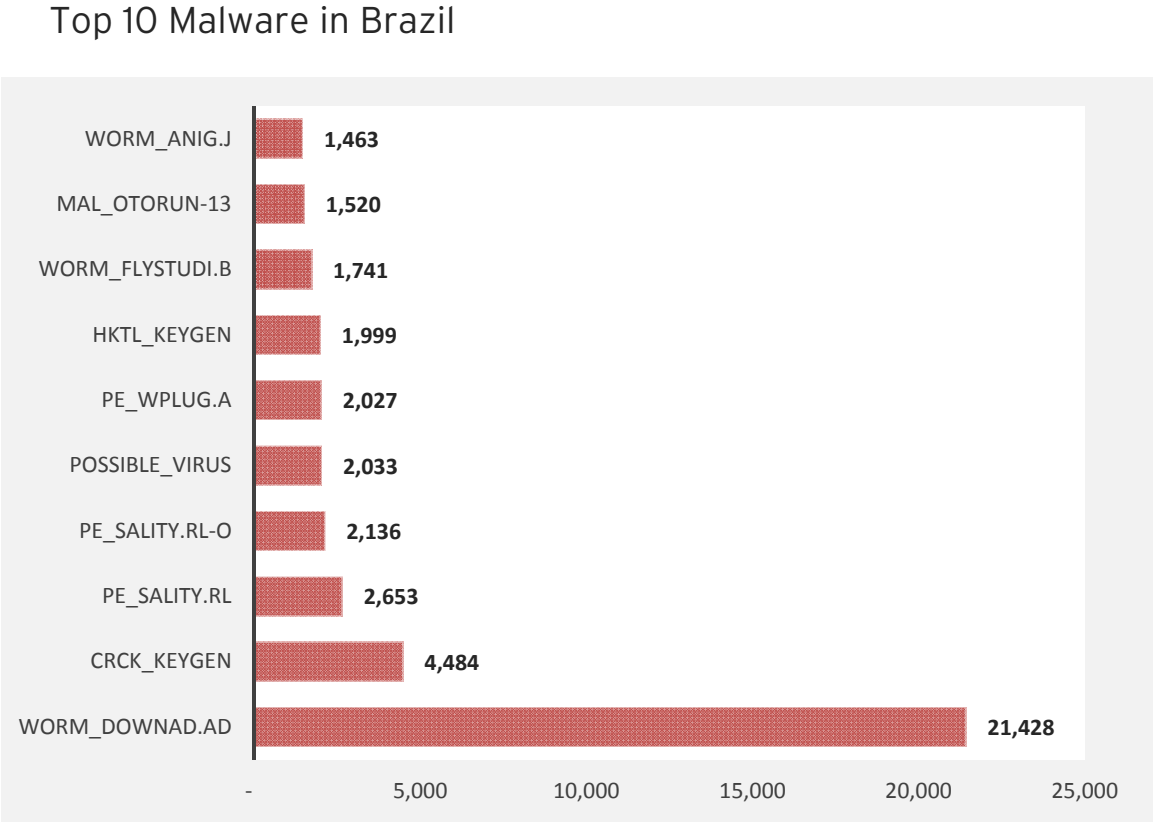
24 Robert Bruce, et al. (June 30, 2005). "International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues." Last accessed June 24, 2013, http://www.ists.dartmouth.edu/library/158.pdf.

25 Computer Security and Incident Response Team. (February 27, 2013). "About Us." Last accessed June 24, 2013, http://www.ctir.gov.br/sobre-CTIR-gov.html.

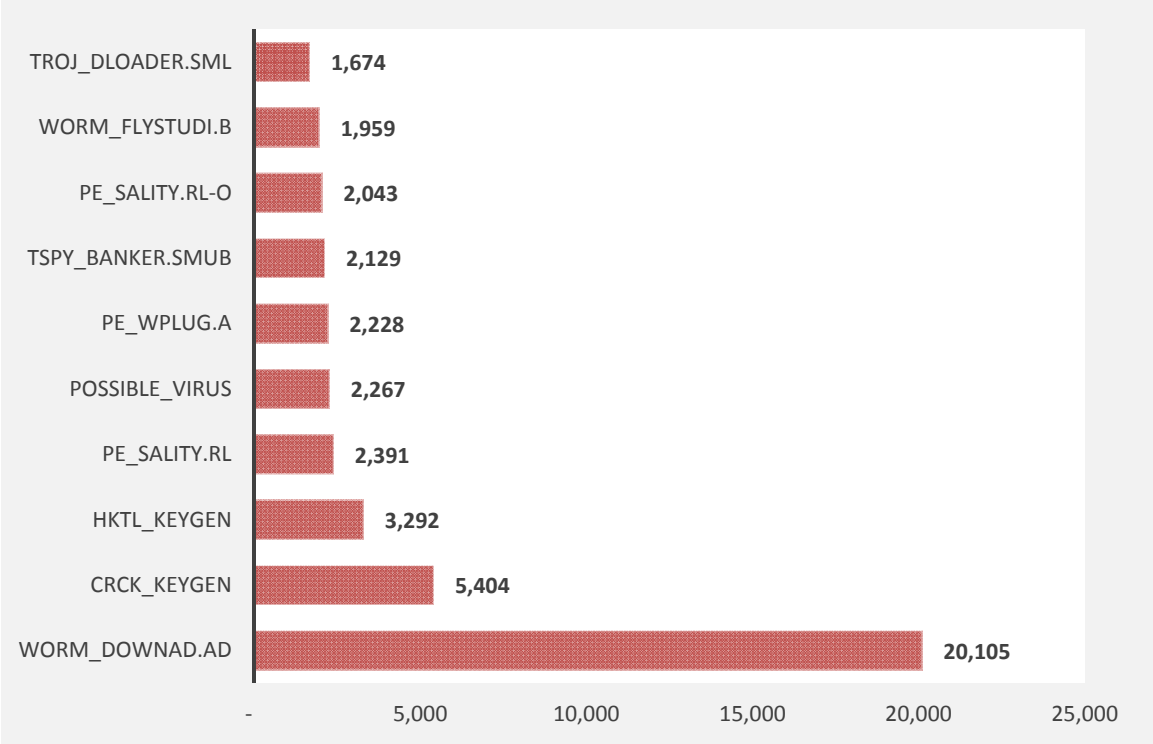
26 Steering Committee of Information Security. (June 24, 2013). "About Us." Last accessed June 24, 2013, http://dsic.planalto.gov.br/quem-somos; "Decree 3505 of June 13, 2000." Last accessed June 24, 2013, http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm.

27 Computer Emergency Response Team Brazil. (June 5, 2013). "About Us." Last accessed June 24, 2013, http://www.cert.br/en/.

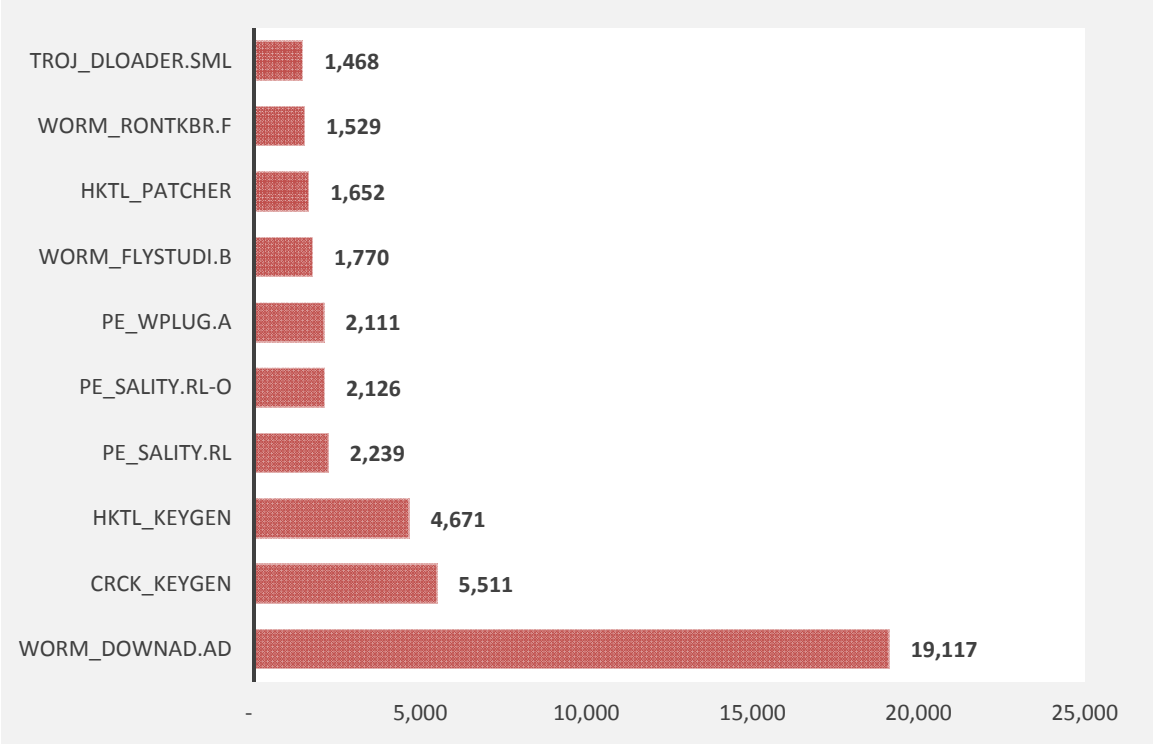
5. **Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC)/Center for Research and Development Safety Communications:** This is an R&D center tasked to support the Executive Secretary of the National Defense Council's activities related to information security and handle teams and groups for advisory assignments.



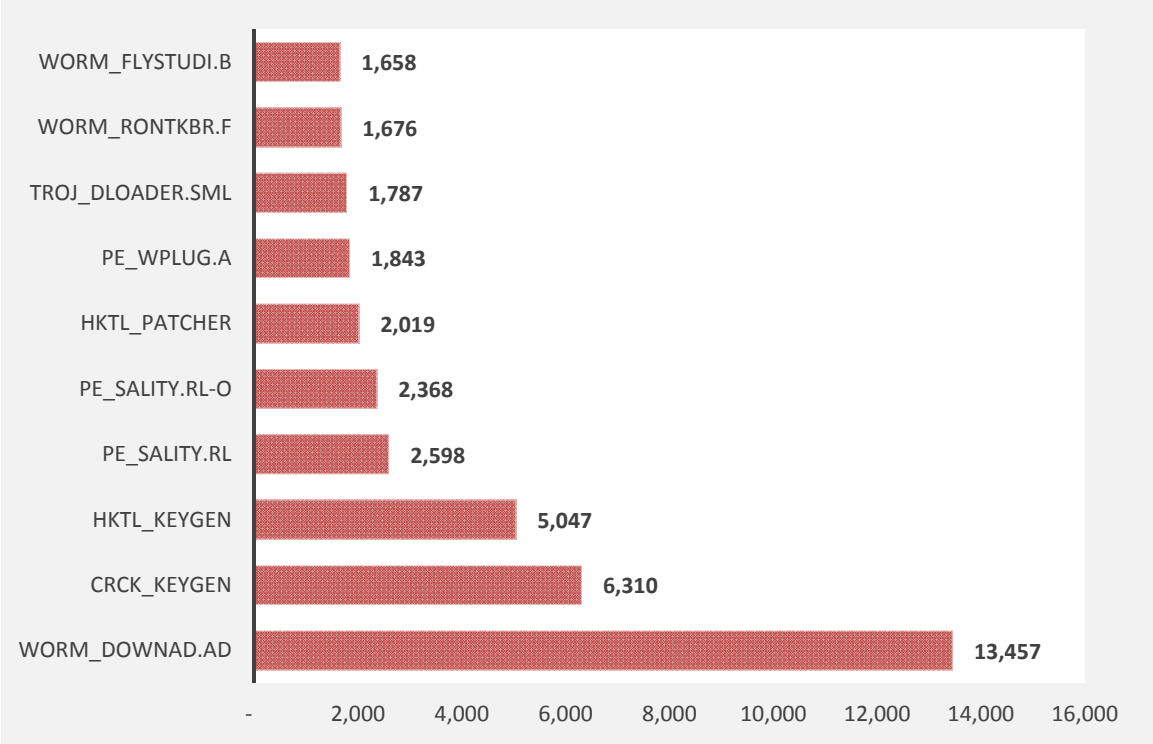
Top 10 malware in Brazil, 1Q 2012



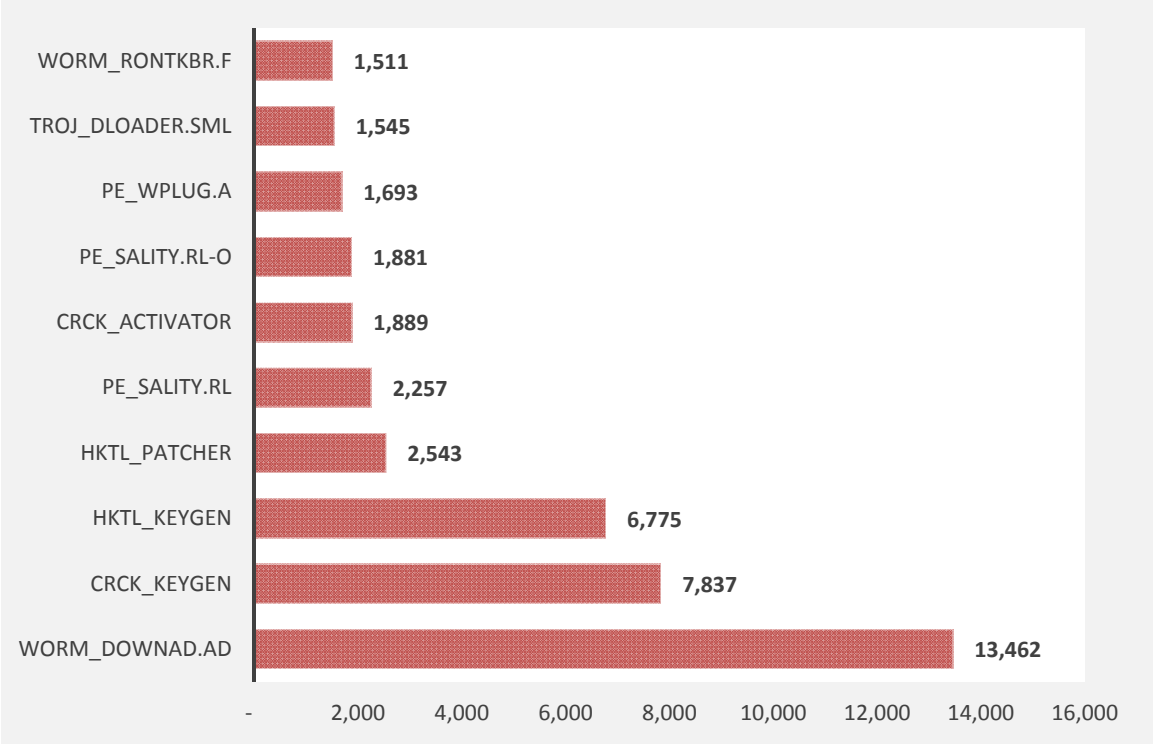
Top 10 malware in Brazil, 2Q 2012



Top 10 malware in Brazil, 3Q 2012



Top 10 malware in Brazil, 4Q 2012



Top 10 malware in Brazil, 1Q 2013

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.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003