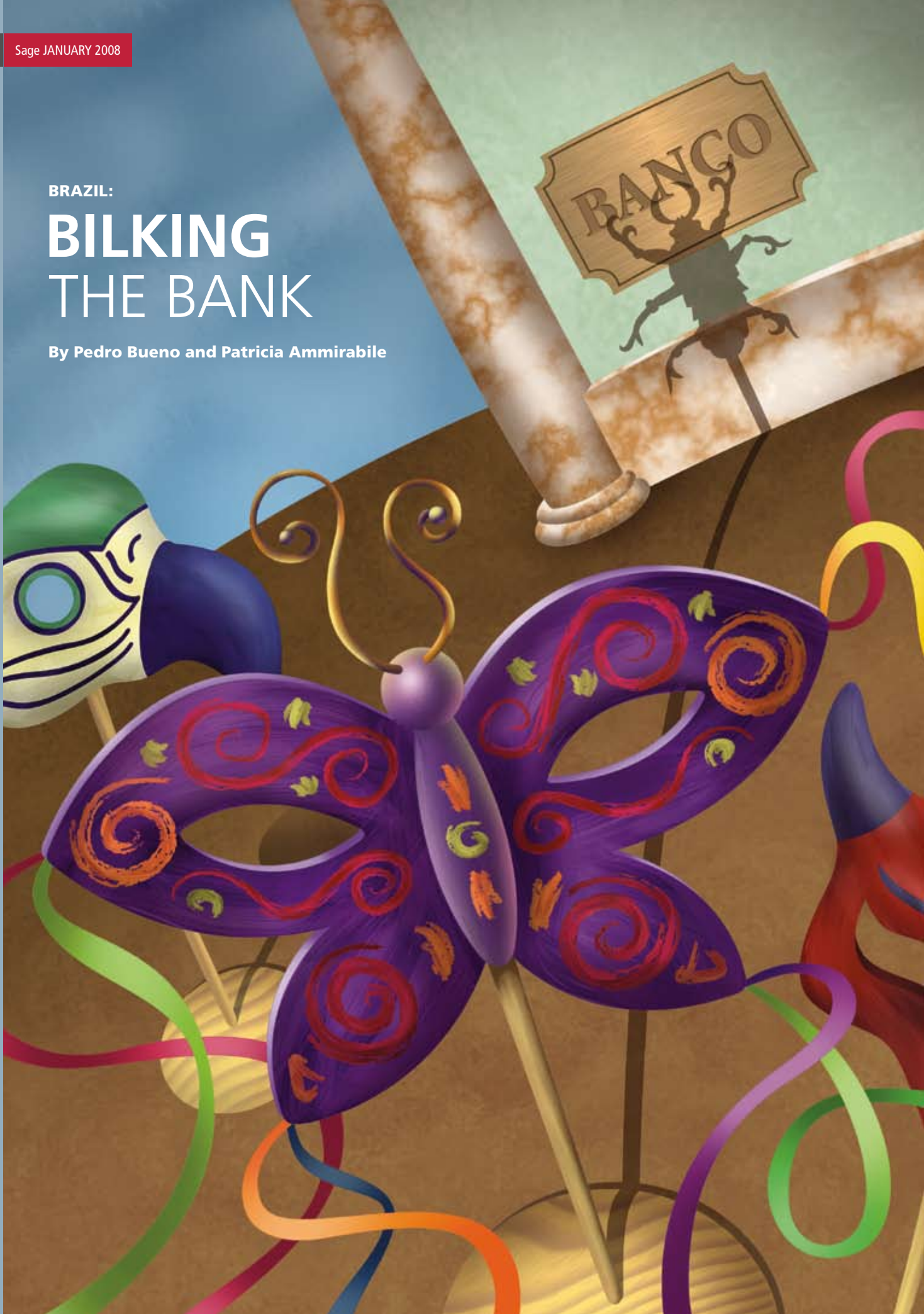


BRAZIL:

BILKING THE BANK

By Pedro Bueno and Patricia Ammirabile



Cybercrime has a significant economic impact that varies around the world. Further, the types of cybercrime can differ significantly from country to country. In South America, Brazil has been suffering for some years from a plague of Trojans called PWS-Bankers. The PWS stands for password stealers, so this malware specifically targets bank account passwords.

The Trojans invade via phishing scams. These fake e-mails turn thousands of users into victims in Brazil, and abroad, year after year, by displaying fake login pages and playing mind games with the victims. One trick is to exploit a victim's willingness to help others by appealing for help after disasters such as hurricanes, air crashes, and more.

In Brazil, the finance industry—by a wide margin—is the preferred target of cybercrime. In 2005 alone, Febraban (the Brazilian Banks Federation) estimated the losses at R\$300 million (reais, about US\$165 million) due to virtual fraud in Brazil.

In this paper we will look at how Brazilian banks are organized, how the password stealers work, and the efforts of Brazilian federal police.

The State of Online Banking

According to Febraban, "Brazilian banks are concerned with this new fraud/hacking scenario, but they are aware that the technology innovation has gone past the point of no return, either due to the evident benefits to customers—who gain time and convenience for transactions anywhere, anytime—or to the sheer efficiency gains provided by the new channels to the Brazilian financial system. That's why so much is invested to enhance banking technology: R\$4.2 billion [US\$2.3 billion] in 2003 and R\$6 billion [US\$3.3 billion] in 2006."¹

As result of these actions, Brazil today has one of the most efficient and secure online banking systems. Almost 100 percent of Internet banking sites use HTTPS and two PINs (one to log into the system and the other to confirm an operation). Some banks are using "paper token" and OTP (one-time password) tokens to provide another layer of security.

To understand how the PWS-Bankers manage to work around this security, we must first understand how the Internet banking system works.

Here are the basic steps to log into a Brazilian bank:

- User goes to the HTTP bank site
- Inserts the branch office and account numbers
- User is redirected to HTTPS site
- User enters the Internet PIN (or token number)
- User starts a transaction, such as a money transfer
- User enters the bank PIN/token number to confirm

How do PWS-Bankers work?

One of the factors that has led to the increase in the number of online scams is the sophistication of the messages sent to users. These are very different from the early days of phishing messages, which often contained grammatical mistakes and typos, as well as inappropriate language. The latest scams lure users by showing a legitimate look and high-quality images; phishers also send near-perfect copies of texts used by respected companies. Attack tools are even available from the online underground market, allowing "lamers" (hackers with only basic technical skills) to participate in online fraud.²

Phishing emails arrive at a victim's mailbox with one of a variety of subjects:

- Fake orders from well-known Brazilian online stores
- Fake greeting cards
- Fake sex pictures/videos of celebrities
- Fake tax software
- Fake election reports
- Fake pictures of car/airplane crashes

¹ "Segurança" (in Portuguese), Febraban. http://www.febraban.org.br/seguranca_site/seg_compromisso_de_todos.asp
http://www.febraban.org.br/seguranca_site/seg_investimento_seguranca_2007.asp

² "Lamer," Wikipedia. <http://en.wikipedia.org/wiki/Lamers>

The emails contain links that lead victims to download PWS-Bankers.dll, which are the downloaders of PWS-Bankers. The malware writers cleverly use these small downloaders, which are around 45KB or less, to prevent users from becoming suspicious. Once aboard, the small applications quietly download the real PWS-Banker, which is about 1MB–4MB, in the background.

Once PWS-Banker is installed, it sends a background email to its author to confirm that another machine has been infected. The hacker gains the following information:

Computer Name: MACHINE-SVR
 Computer User: Administrator
 IP: 192.168.241.100
 Date: 9/6/2007 Hour: 7:19:03 AM
 Windows: Microsoft Windows XP (Version 5.1)
 Mac Address: 00-0C-29-3C-C7-A1
 IE-Version: 6.0IE-Version: 6.0.2600.0000
 Windows Key: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

PWS-Banker will remain resident in the memory, monitoring the web sites the user visits. The malware usually has a list of five to eight banks to target. When PWS-Banker notices

the user request the URL of one of these banks, it will pop up a fake window that mimics the bank's site.

Most banks in Brazil ask for account number, branch office number, and Internet PIN to allow the user to log in. The Trojan will ask for some additional information: the bank PIN, and credit card number, verification code, and expiration date, among other data.

Once the malware has this information, it will display an error message and redirect the user to the bank's true Internet page, while sending an email to the hacker with all the information:

- Account name
- Account number
- Internet PIN
- Bank PIN
- Pass phrase
- Account owner's name
- Credit card number
- Credit card PIN
- Credit card date
- Credit card expiration date
- Father's name (for positive authentication)

These examples illustrate the differences:

Figure 1: A real bank's online screen. A genuine bank asks only for user name and Internet PIN.

Figure 2: Fake screen used by the PWS-Banker Trojan. This form digs a little deeper, asking the user for branch office number, account number, and bank PIN.

Quick Update by PWS-Bankers

On June 16, 2007, the major corporation Banco do Brasil released a new Internet banking web site, updating everything in its design. Banco do Brasil is one of the most targeted banks in the country, and most PWS-Bankers already had a copy of the bank’s old web design inside their databases of fake banks.

With a few days we discovered a source-code repository of PWS-Bankers, and found plenty of files that targeted Brazilian banks. One file in particular caught my attention; it was called “New Banco do Brasil Screen.jpg.” This file had the date June 21 and had the brand new password screen of the new Banco do Brasil web site! Assuming that the dates are accurate, in fewer than five days the miscreants had a functional PWS-Banker Trojan that was ready to pose as the new bank site.

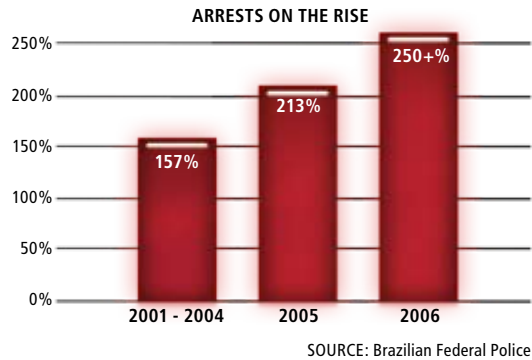


Figure 3: The Brazilian police arrested more malware writers in 2005 than in the four previous years combined. Arrest figures in 2006 continued that increase.

The federal police are enjoying some success in their contest with hackers. In the period from July to September 2007, police arrested almost 100 persons involved with bank-account password stealers.

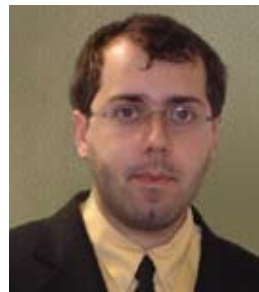
In July the police operation Nerds II led to the capture of 29 persons alleged to be responsible for the deviation of more than R\$10 million (US\$5.5 million) in less than one year.

Conclusion

In spite of the increase in phishing and password-stealing Trojans, Brazilians enjoy reasonably strong security for online banking. Nonetheless, the struggle against malware is ongoing.

We can recommend a number of best practices for both consumers and corporations. The business methods include establishing policies for email, web browsing, and effective security software. Consumers should employ software to block spam, spyware, and outbound data to malicious sites. And it pays to be suspicious: If you aren’t sure whether an email is legitimate, call the apparent sending institution to verify its authenticity.³

The coordinated efforts of financial institutions, federal police, security software companies and end-user education are making progress in containing and diminishing the current large volume of criminal activities that target online banking.



Pedro Bueno is a Virus Research Engineer at McAfee® Avert® Labs in Brasília. He has worked more than 10 years in the security arena,

managing incidents for large telecom companies and serving as a volunteer handler at the SANS Internet Storm Center.



Patricia Ammirabile is a Virus Research Analyst with McAfee Avert Labs in São Paulo. She has worked at McAfee for 12 years;

her duties have included offering high-level technical support to both corporate and home users, providing multilingual and translation services, and analyzing malware.



3 “Anti-Phishing: Best Practices for Institutions and Consumers,” McAfee. http://www.mcafee.com/us/local_content/white_papers/wp_anti_phishing.pdf