

February 27, 2006

Cyberthieves Silently Copy Your Passwords as You Type

By [TOM ZELLER Jr.](#)

Most people who use e-mail now know enough to be on guard against "phishing" messages that pretend to be from a bank or business but are actually attempts to steal passwords and other personal information.

But there is evidence that among global cybercriminals, phishing may already be passé.

In some countries, like Brazil, it has been eclipsed by an even more virulent form of electronic con — the use of keylogging programs that silently copy the keystrokes of computer users and send that information to the crooks. These programs are often hidden inside other software and then infect the machine, putting them in the category of malicious programs known as Trojan horses, or just Trojans.

Two weeks ago, Brazilian federal police descended on the northern city of Campina Grande and several surrounding states, and arrested 55 people — at least 9 of them minors — for seeding the computers of unwitting Brazilians with keyloggers that recorded their typing whenever they visited their banks online. The tiny programs then sent the stolen user names and passwords back to members of the gang.

The fraud ring stole about \$4.7 million from 200 different accounts at six banks since it began operations last May, according to the Brazilian police. A similar ring, broken up by Russian authorities earlier this month, used keylogging software planted in e-mail messages and hidden in Web sites to draw over \$1.1 million from personal bank accounts in France.

These criminals aim to infect the inner workings of computers in much the same way that mischief-making virus writers do. The twist here is that the keylogging programs exploit security flaws and monitor the path that carries data from the keyboard to other parts of the computer. This is a more invasive approach than phishing, which relies on deception rather than infection, tricking people into giving their information to a fake Web site.

The monitoring programs are often hidden inside ordinary software downloads, e-mail attachments or files shared over peer-to-peer networks. They can even be embedded in Web pages, taking advantage of browser features that allow programs to run automatically.

"These Trojans are very selective," said Cristine Hoepers, general manager of Brazil's Computer Emergency Response Team, which runs under the auspices of the country's public-private Internet Steering Committee. "They monitor the Web access the victims make, and start recording information only when the user enters the sites of interest to the fraudster." She added: "In Brazil, we are rarely seeing traditional phishing."

According to data compiled by computer security companies in 2005, the use of "crimeware" like keyloggers to steal user names and passwords — and ultimately cash — has soared. The crimes often cross international borders, and they put Internet users

everywhere at risk.

"It's the wave of the future," said Peter Cassidy, the secretary general of the Anti-Phishing Working Group, a consortium of industry and law enforcement partners that fights online fraud and identity theft. "All this stuff is becoming more and more automated and more and more opaque."

Mr. Cassidy's group found that the number of Web sites known to be hiding this kind of malicious code nearly doubled between November and December, rising to more than 1,900. The antivirus company Symantec has reported that half of the malicious software it tracks is designed not to damage computers but to gather personal data. Over the course of 2005, iDefense, a unit of Verisign that provides information on computer security to government and industry clients, counted over 6,000 different keylogger variants — a 65 percent increase over 2004. About one-third of all malicious code tracked by the company now contains some keylogging component, according to Ken Dunham, the company's rapid-response director.

And the SANS Institute, a group that trains and certifies computer security professionals, estimated that at a single moment last fall, as many as 9.9 million machines in the United States were infected with keyloggers of one kind or another, putting as much as \$24 billion in bank account assets — and probably much more — literally at the fingertips of fraudsters. John Bambenek, the SANS researcher who made the estimate, suggested that the infection rate was probably much higher.

In most cases, a keylogger or similar program, once installed, will simply wait for certain Web sites to be visited — a banking site, for instance, or a credit card account online — or for certain keywords to be entered — "SSN," for example — and then spring to life.

Keystrokes are saved to a file, Web forms are copied — even snapshots of a user's screen can be silently recorded. The information is then sent back to a Web site or some waiting server where a thief, or a different piece of software, sifts through the data for useful nuggets.

The Federal Deposit Insurance Corporation, responding to the growing threat of cybercrime to the financial industry, stiffened its guidelines for Internet banking in October, effectively ordering banks to do more than ask for a simple user name and password. But it stopped short of requiring, for instance, the use of electronic devices that generate numeric passcodes every 60 seconds, which many experts say would help foil much online fraud, including the use of keyloggers.

Technology for grabbing text and screen images is not new — or particularly sophisticated. Keyloggers are even sold commercially, as tools for keeping an eye on what children are doing online, or what a spouse might be doing in online chat rooms. And while most experts agree that data-swiping software is spreading rapidly, there are some who say the problem has been exaggerated.

"I get concerned that we're scaring people off the Internet," said Alex Eckelberry, the president of Sun-Belt Software, a maker of antispyware software based in Clearwater, Fla. Mr. Eckelberry believes that the infection rate is probably far lower than most estimates indicate, in part because the trend is hard to measure and so many computers are already protected.

"There's a lot of hyperbole out there," he said, adding that his company has identified only about 30 keyloggers over the last six months, most being variations on a piece of code known as Winldra.exe.

That code proudly bears the copyright signature of its creators, "Smash and Sars," who also happen to be the proprietors of a

Russian site, RATSystems.org, which is well-known among traders at online swap meets like theftservices.com and carders.ws/forum that traffic in confidential personal data — or the means to steal it.

"Smash is one of the revolutionaries," said one member of a trading site, who insisted on anonymity because the sites are often watched by law enforcement. "If you're entry-level and want a keylogger, that's who you're going to go to," he said, adding, "It's a simple, cheap way to make money."

In fact, keylogging's simplicity may be why it is suddenly so popular among thieves. "Phishing takes a lot of time and effort," said David Thomas, the chief of the computer intrusion division at the Federal Bureau of Investigation. "This type of software is a much more efficient way to get what they're after."

The programming, too, is often trivial. "These can be developed by a 12-year-old hacker," said Eugene Kaspersky, a co-founder of Kaspersky Labs, an international computer security and antivirus company based in Moscow.

Being wary of unfamiliar Web links sent via e-mail is a first-line of defense, according to experts, as is avoiding questionable downloads and keeping up to date with Windows patches and antivirus updates.

It is worth noting, however, that in a test of major antivirus programs conducted by Ms. Hoepers's group in Brazil last fall, the very best detected only 88 percent of the known keyloggers flourishing there. In this country, victims of fraudulent money transfers are typically limited to \$50 in liability under the Federal Reserve's Regulation E, so long as they report the crime quickly enough — within two days. If they report it within 60 days, their liability is capped at \$500.

One Florida man has had trouble getting that kind of protection. In a closely watched case, Joe Lopez, the owner of a small computer supply company in Miami, sued Bank of America after cybercrooks were able to use a keylogging Trojan planted on his business computers to swipe bank account information and transfer \$90,000 to Latvia.

Bank of America says it does not need to cover the loss because Mr. Lopez was a business customer — and because it is not the bank's fault that he did not practice good computer hygiene. Mr. Lopez claims he did, and that in any case, Bank of America should have done more to warn him of the risks of computer crime. That risk is one that Mr. Kaspersky believes is in danger of getting out of hand.

"I'm afraid that if the number of criminals grows with this same speed, the antivirus companies will not be able to create adequate protection," said Mr. Kaspersky, who added that the time has come for increased investment in law enforcement and far better cross-border cooperation among investigators, who are overwhelmed by the global nature of cybercrime.

"There are more criminals on the Internet street than policemen," he said.

[Copyright 2006 The New York Times Company](#)

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [XML](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)