



Forget phish, start fumigating for RATs

'Remote access Trojans' harvest online bank passwords as you type them

By **Bob Sullivan**

Technology correspondent

MSNBC

Updated: 3:20 p.m. ET Nov. 2, 2005

Forget phish. It's rats that are about to cause the most trouble for Internet users.

Clever computer criminals have recently become much more sophisticated in their attacks against online banks, experts say. The Internet is now awash in programs called "remote access Trojans," or RATs, that feed on online banking passwords.

Trojan horse programs have traditionally sneaked their way onto computers by posing as desirable free software, such as electronic greeting cards or file-sharing programs. The malicious programs are hidden, and like the Greek soldiers hidden in the famous wooden horse, jump out to attack once they're safely inside. But others are pushed onto computers without any interaction at all, through various software vulnerabilities. In that case, consumers would likely have no way of knowing their machine has been subdued.

These new remote-access Trojans are designed specifically to lurk in the background, waiting until the unsuspecting user types the name of a well-known bank into a Web browser. Then, the program springs into action, copying every keystroke. The data is sent back to the criminal, who now can raid the online bank.

"This is the new thing," said Dan Clements of CardCops.com, a site that monitors online fraud. His researchers recently gained access to an e-mail account that was set up to receive data from RAT-infested computers. The account held over 3,000 transmissions, he said.

One of the e-mails contained about 300 logins for Bank of America's Web site.

"I get more and more of these every day," he said. "(Researchers) send it to me and say, 'Why isn't anybody doing anything?'"

Bank of America's Betty Riess said she couldn't comment on the specific case, but said the bank is currently rolling out new security features designed to limit the effectiveness of Trojan horses.

Generally, banks are loath to discuss fraud, so there is precious little hard data about its extent. But the Antiphishing Working Group, a consortium set up by financial firms and security companies, has noticed a dramatic uptick in RAT programs, says spokesman Dave Jevans.

Last month, the agency detected 170 distinct Trojan programs used to steal bank data. In January, there were only about 30, he said.

"It's quite a big change," he said. "(Banks) are having a hard time dealing with it, frankly."

Sneak attacks

These specialized forms of spyware, now being called by other names like crimeware, ratware, and even

bankware, worm their way onto victims' computers in a number of ways. Some are inserted completely in silence, through an unpublished or unpatched software vulnerability. Others are hidden in Web sites on the Internet's darker side, such as pornography sites. Still others come in e-mail, disguised as electronic greeting cards.

But unlike familiar computer worms, these malicious programs do nothing to announce their presence — like send out copies of themselves to everyone in the victim's address book. Instead, they lie in wait for the user to visit a banking Web site.

Security companies agree that such Trojans are popping up everywhere. Richard Stiennon spokesman for anti-spyware maker Webroot, said his firm's research indicates that 1 in 10 Internet-connected computers has a Trojan horse installed on it. While many of those infected computers are still protected by firewalls that prevent data from being sent outside the system, others are at immediate risk, Stiennon said.

"Of all the threats we track, only one is increasing its presence in the enterprise: Trojan horses," he said. "For harvesting (personal) information it's more successful than phishing attacks."

Avivah Litan, an online banking security consultant at Gartner Inc., says banks are starting to feel the effects of the silent programs, even though there has been little public discussion about them. The very stealth nature of the programs has kept publicity about the trend at a minimum.

"No one has to talk about this because no one sees it," she said. "But I've definitely heard about it from major clients. ... They can tell from their consumers' calls to call centers."

Has phishing peaked?

Antivirus companies paint much the same picture. Once upon a time, viruses written by fame-seeking malcontents were designed to infect as many computers as possible. Now, viruses are designed to infect the right computers and to do so quietly — all with the aim of spiriting off valuable data that can be used to steal money.

Three-quarters of all virus-like programs released to the Internet this year have been designed to steal personal information, said Oliver Friedrichs, a spokesman for Symantec Corp. Last year, the rate was 36 percent.

In fact, there have been only five widespread virus attacks so far this year, down from 33 last year.

"Attackers are increasingly using new technology," he said. "It is a problem and people are being affected by it."

Why the shift to ratware? There is some evidence that phishing activity has finally peaked. Jevans said the number of phishing attacks in September leveled off. Consumers may have finally gotten the message that e-mails which appear to be from major financial institutions are often fakes; so criminals have upped the ante, shifting their attention to these more sophisticated methods that don't require a consumer mis-step.

The trend hasn't escaped the notice of law enforcement. In October, [Dutch police announced the arrest of three men](#) —including one teen-ager — who had allegedly amassed an army of 100,000 computers using a Trojan named Toxbot. And last week, the Federal Trade Commission and Microsoft announced a public education campaign around zombie computers.

But the would-be criminals, apparently, are bold. On one Web site that claims to sell such ratware, the list of program features sounds impressive. A few claims:

- "This kind of viruses grabbs {sic} all possible info from victims PC and sends it to the owner of the virus."
- "This technology shows how it's easy to make MS Windows think what there is no your program on PC. It makes program process invisible for Task Manager and other similar programs."
- "This technology shows few FireWalls leaks which allow to bypass notifications and rules while spyware application connecting to remote host. With this technology you can bypass about 70-80% of all personal FireWalls."

According to the site, the program sells for \$650. Site authors didn't immediately respond to requests for information. While it's not clear that site is really selling anything, experts agree the technology is out there, and being used to attack consumers and computers.

New security technology takes up the fight

That's part of the reason federal regulators instructed banks last month to come up with new, better ways to authenticate consumers — methods that go beyond use of a simple user name and password that can easily be stolen. The Federal Financial Institutions Examination Council gave banks until next year to come up with improved methods.

Riess said Bank of America is already testing improved security in California. If a customer tries to access its site from a computer that's not their usual haunt, the Web site interrupts to ask a set of personal questions, such as "What was your first's pet's name?" The answers are supplied by the customer beforehand, when setting up the account.

Such personal questions wouldn't stop the most determined of criminals — with a RAT program installed, the criminal could have spied the answer months earlier — but would raise the bar against criminals that simply steal user names and passwords.

Dutch banking conglomerate ING has another anti-keystroke logging technology on its Web site. Consumers have to type their pins by clicking with their mouse on a number keypad displayed on a Web page. Such clicks can't be tracked by keyloggers.

But Gartner expert Litan says criminals have managed to stay one step ahead, and there's no reason they won't continue to up the ante. The next step for RAT programs is continuous screen capture, which would allow a criminal to watch every move a consumer makes online, as if peeking into the room with a video camera. The technology already exists, but it is bandwidth intensive -- a problem that's slowly disappearing as consumers sign up for higher-bandwidth services. ING's system would be easily foiled by continuous screen captures.

"If you put up a 10 foot wall, they're going to find an 11-foot ladder," says CardCops' Clements. "And consumers don't even know this is going on."

Bob Sullivan is author of [Your Evil Twin: Behind the Identity Theft Epidemic](#).

© 2005 MSNBC Interactive

© 2005 MSNBC.com

URL: <http://www.msnbc.msn.com/id/9898957&&CM=EmailThis&CE=1/>