

washingtonpost.com

Cyber-Criminals and Their Tools Getting Bolder, More Sophisticated

By Brian Krebs
washingtonpost.com Staff Writer
Wednesday, March 14, 2007; D02

Robert Hoyler thought hackers who broke into his computer stole only his bank account information. But it turned out that the thieves also left something behind: a hidden software virus that recorded his every keystroke.

So when Hoyler's bank issued him new account numbers and passwords, the hackers got all that information, too. His health insurance, online shopping and Social Security data went into a file in a master database at a Web site controlled by the attackers, stashed among personal information on more than 3,220 U.S. residents.

"These guys got everything, but all I knew was that my financial accounts were compromised," said the 66-year-old Fairfax engineer, who learned of the virus from a reporter who used forensic tools from computer-security firm Sunbelt Software in February to locate the Web server hosting Hoyler's private information.

Such attacks are evidence of the sophistication and depth of technical manipulation by hackers, and the challenges facing consumers and law enforcement agencies in fighting them.

Online crime is easier, in part because tools for carrying out attacks are readily available and harder to purge from computers. Moreover, for consumers like Hoyler, there is often no surefire way to know how or what information has been stolen. Notifying individual victims is time-intensive and expensive, and law enforcement agencies and credit bureaus say it's not their job.

Many viruses that send junk e-mail also include password-stealing components, and some combine such technology with fake Web sites mimicking trusted online brands, which can be particularly deceptive. More than 1,000 fraudulent sites known as "phishing" sites are erected each day, according to the Anti-Phishing Working Group, an industry organization. Scammers can net 20 to 100 victims per case, according to CastleCops, a volunteer group of security experts that analyzes malicious software and phishing sites and provides information to police, Internet service providers and affected companies.

Contributing to the proliferation of Web-based crime is the broad availability of online tools.

"Basically we're at the point where the scammer can go into the virtual tackle store and buy all the equipment he needs to get a phishing scam working," said Lance James, founder of security-software developer Secure Science. "There's the guy who writes the [virus] who says, 'Here's your phishing rod, here's some of our best bait, here are the best sites to attack, and if you pay me an extra \$200, I'll tell you some of the best sites you can hack into.' "

The virus that stole Hoyler's information came from Web sites based in Eastern Europe, according to the information tracked by Sunbelt Software. It infiltrated the new-accounts department of a major U.S. bank, a medical patient database in Georgia and an Alabama district attorney's office containing a database used by police departments to trace people, according to information obtained with the Sunbelt software.

Hoyler's bank told him in January that someone had tried to wire money out of his account. Days later, Fidelity Investments notified him that someone tried to use his log-in information to purchase thousands of shares of an adult-entertainment company.

Advertisement

Play a free round
of golf on the
world's finest
courses.

* Free with qualifying trip
and Frequent Flyer
Program membership.

Subject to terms and
conditions

Better get
practicing!



The government has acknowledged a need to do more for identity-theft victims. Last year, the Bush administration created an identity-theft task force that has proposed creating a center that would help victims.

Federal law enforcement officials said they routinely provide data they uncover on compromised credit and debit accounts to MasterCard, Visa and other credit-card issuers. The FBI also said it recently began sharing caches of stolen consumer data with the fraud departments of the three major credit-reporting bureaus.

But because credit-card companies often do not get any more information about the extent of the breaches, victims of viruses or scams may think that their problems have been resolved after being issued new credit or debit cards. And such agencies as the FBI handle too many incidents to notify online crime victims individually.

"We're just getting overwhelmed with this [compromised] consumer data, but it's not exactly law enforcement's job to call each victim and explain the situation," said Dan Larkin, an FBI agent who heads the National Cyber-Forensics & Training Alliance in Pittsburgh.

Credit bureaus are not required to notify consumers.

"The credit bureaus work on behalf of banks and companies that grant credit," said Ari Schwartz of the Center for Democracy and Technology, a consumer advocacy group in Washington. "They're not set up to be consumer-oriented businesses."

And the credit bureaus say they are not in the habit of reaching out to consumers whose private information may have been compromised.

"Normally we would not put a fraud alert on a file without a consumer being involved" or initiating it, said Maxine Sweet, a vice president with Experian, one of the three major credit-reporting bureaus. "That's just not something we generally do."

© 2007 The Washington Post Company

Ads by Google

[Find a Military Buddy](#)

at an Armed Forces Reunion Find your group online

www.afri.com

[Free dating and reunion.](#)

Singles, Classmates and Military Friends. All at one website.

www.foundyouonline.com

[All Military Records ®](#)

Find any Military Record in 1 Min. Using The Database of Government!

Gov-Records.com