



Botnet Herder Pleads Guilty to Massive PayPal Scam

November 12, 2007

By Lisa Vaas

A 26-year-old security consultant named John Schiefer has admitted to illicitly installing code to assemble botnet armies of up to 250,000 infected computers that harvested user PayPal names, passwords and other personal and financial information.

In this, the first prosecution of its kind in the nation, the Los Angeles man will plead guilty to four felony counts: accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud.

Schiefer filed his plea agreement on Nov. 9, according to a statement from the U.S. Attorney's office for the Central District of California.

ADVERTISEMENT

 An advertisement for Trend Micro. It features a smiling man in a white shirt and red tie. The Trend Micro logo is in the top right. The main text reads "My network is secure." in red, followed by "Is yours?" in grey. At the bottom, a red curved button says "download FREE Web Threats white paper >>".

RELATED LINKS

- [Storm Worm Botnet Lobotomizing Anti-Virus Programs](#)
- [PayPal Security Chief: User Education Remains Greatest Hurdle](#)
- [Botnet Attack Sinks Its Fangs into eBay Accounts](#)
- [How Botnets Are Lobotomizing Your PC](#)
- [Keeping an Eye on Botnets](#)

The charges detail a series of schemes in which Schiefer and several others developed and distributed malware to vulnerable computers. The code rendered the victimized systems into zombie computers that were then marshaled in armies of up to a quarter million strong and used to carry out a variety of

identity theft scams. Schiefer is also charged with using the zombie PCs to defraud a Dutch advertising firm.

Schiefer and his associates listened in on the compromised systems to intercept communications from their unwitting users to PayPal and other Web sites. With the PayPal user names and passwords in hand, Schiefer and his gang waltzed into victims' bank accounts to make purchases, unbeknownst to the true owners of the accounts.

For more on how botnets lobotomize your PC, listen to your podcast.

Schiefer also admitted to transferring the intercepted information and stolen PayPal accounts to others.

Schiefer and his gang also admitted to installing malware on Windows systems, causing them to cough up user names and passwords from a supposedly secure storage area known as [PStore \(Protected Storage\)](#), an area used to store user data to keep it secure or free from modification—an obvious sweet spot for identity thieves. PStore is known to be a less-secure method of storage than Microsoft's DPAPI (Data Protection API) and has been deprecated and made read-only in Windows Vista.

Schiefer is also admitting to defrauding an Internet advertising company with his botnets. He was serving as a consultant with a Dutch Internet advertising company and promised to install the company's programs on computers only when the owners gave consent. Instead, Schiefer and two co-schemers installed that program on approximately 150,000 computers that they had previously infected with their malware.

To avoid detection by the advertising company, Schiefer instructed his associates to moderate the number of installations so it appeared that the installations were legitimate and not the result of a malicious computer program. Schiefer was ultimately paid more than \$19,000 by the advertising company.

Schiefer is facing a statutory maximum sentence of 60 years in federal prison and a fine of \$1.75 million.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

This is the first time that someone has been charged under the U.S. federal wiretap statute for conduct relating to botnets.

[Copyright \(c\) 2007Ziff Davis Enterprise Inc. All Rights Reserved.](#)