

## 19-year-old p2p botnet pioneer agrees to plead guilty

The author of a Trojan that broke new ground by incorporating peer-to-peer technology into botnet design has agreed to plead guilty to secretly infecting thousands of victims' machines so that he could steal their personal data and launch attacks on websites.

Jason Michael Milmont, 19, of Cheyenne, Wyoming, admitted to creating the so-called Nugache Worm, a Trojan that spread through AOL instant messenger and modified Limewire installation programs. Once clicked on, the malware made unwitting users part of a botnet, which Milmont used to steal user names, passwords and account numbers of those who were infected.

Nugache was being circulated as early as early 2006 and spawned one of the first botnets to use a decentralized system to send instructions to drones, according to security researcher Dave Dittrich. Rather than relying on a single command and control channel, the zombie network used a peer-to-peer mechanism to communicate. Such technology fundamentally changed the cybercrime landscape by making it much harder to shut down botnets. (Later botnets such as Storm went on to use a different method to thwart shut down. So-called fast flux technology used DNS records to obscure where central command-and-control channels were located.)

Over time, Milmont added new features to Nugache. A graphical user interface made it easy to access infected machines from his home server. It allowed him to issue a command to a single machine, which would then transmit the command to other machines, until it had spread through the entire network. The program contained a keylogger and was also capable of sniffing sensitive information stored in Internet Explorer to spare users the hassle of having to remember passwords for online banks and other sensitive websites.

The software was invisible to the Windows task manager in versions NT, XP and 2000. At any given time, Milmont had anywhere from 5,000 to 15,000 machines under his control.

According to a plea agreement signed by Milmont, he used his botnet to launch distributed denial-of-service attacks against an unnamed online business located in the Los Angeles area. The agreement went on to document the way he used personal information he lifted from his victims to fatten his wallet.

After sending a command that instructed infected machines to transmit captured passwords and other information, he would order items online and take control of victims' accounts by changing the addresses and other details that were associated with them. In April 2007, for example, he used stolen credit card information to make a \$1,422 purchase from Hinsite Global Technologies and had items shipped to a vacant residence in the Cheyenne area.

To prevent victims from discovering his scheme, Milmont replaced phone numbers associated with compromised accounts with Skype numbers he created and purchased using credit card data he had harvested from his botnet.

Milmont faces a maximum of five years in federal prison and a fine of \$250,000. He's also agreed to pay almost \$74,000 in restitution. Milmont has agreed to appear in federal court in Cheyenne, where he will plead guilty to one felony charge. The case was brought in Los Angeles and was investigated by the FBI. ®

*This story was updated to correct misstatements about fast-flux techniques used in botnets*

[http://www.theregister.co.uk/2008/06/28/nugache\\_creator\\_plea\\_agreement/](http://www.theregister.co.uk/2008/06/28/nugache_creator_plea_agreement/)