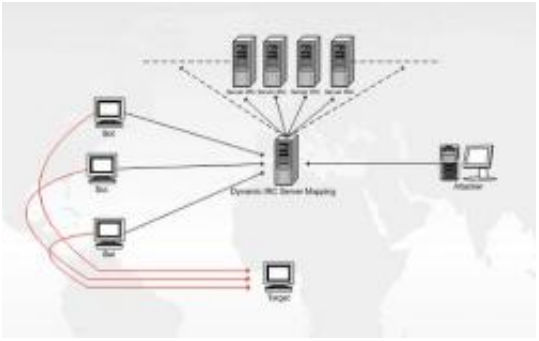
Botnet Hijacking Steals 70GB of Data

May 5 2009, by John Messina



(PhysOrg.com) -- Security researchers have uncovered one of the most notorious zombie networks, the Torpig botnet, by collecting 70GB of data that was stolen in just 10 days.

Torpig bots stole over 8,300 credentials that was used to login to 410 financial institutions. More than 21 percent were PayPal accounts. This brings a total of almost 298,000 unique credentials that were intercepted from over 52,000 infected machines.

Torpig's secret behind siphoning data from computers is by infecting programs such as Mozilla Thunderbird, Microsoft Outlook, Skype, ICQ, and other applications, by monitoring every keystroke. Every 20 minutes, the malware automatically uploads new data to servers. The software is then able to intercept passwords before they may be encrypted by secure sockets layer or other programs.

The security researchers were able to hijack the botnet after discovering weaknesses in the way it updates the master control channels that are used to send new instructions to the infected computers. A technique know as domain flux sporadically generates a large list of domain names of computers to report to but only uses one address, ignoring all the others.

The researchers were able to monitor the botnet's behavior over a period of 10 days by registering one of the domain names on the list and seizing control of the machine. The hijackers eventually gain back control of the machine by using a backdoor built into the infected computer.

In all researchers counted over 180,000 infected computers that connected from 1.2 million IP addresses.

Torpig gains control of a computer by rewriting the hard drive's master boot record. As a result, control of a computer is gained during the early stages of a PC's boot process, allowing it to bypass anti-virus and other security software.