CNS /Update Newsletter Feature

IRC BOTNETs Causing Trouble

CNS Document ID: u040506a
Last Updated: 5/5/2004

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

IRC BOTNETs Causing Trouble .................................................................3
IRC BOTNETs Causing Trouble

IRC (Internet Relay Chat), a system that enables two or more Internet users to conduct online discussions in real time, has become the latest source of network security headaches at UF.

Hackers are using IRC "bots" to channel trojans containing viruses and worms onto unsuspecting Internet users' computers. The term "bot," short for "robot," describes an automated software program that executes commands when it receives specific input.

"Some recent botnets are particularly malicious because they install keystroke logging software compromising user passwords, credit card numbers and other confidential information," UF Information Security Manager Kathy Bergsma said.

Bergsma said that these infected personally controlled computers on the network are causing a recent rash of "botnet" attacks. A botnet attack is when an automated software robot spreads trojans with viruses and worms. Bergsma said that her team will try to notify owners of such computers when they find the computers are infected. "These infected computers can be difficult to locate," Bergsma said. "If we can't find them, we must block their access to the network."

IRC is one of the earliest versions of Internet "chatting," and is still widely used by groups of people with common interests. "Bots" were originally used by IRC members to manage access lists, run quizzes, or serve files. The major difference between these new bots and IRC client script bots is that the botnet variety have been created with a trojan and, almost always, without the knowledge of the person from whose computer they are running.

The trojans get into poorly protected machines and spread to other poorly protected machines in the usual ways: from infected Web sites, spyware, e-mail, or (recently) IRC chat channels. When the infected computer is next connected to the Internet, that trojan will start up an IRC client and connect to a server. Often it is an IRC server which has been set up on a shell account and paid for with a stolen credit card. The trojan will have been coded to make the bot join a certain channel once it has connected.

Once the trojan has infected many computers, the chosen channel will be overrun with the bots. This collection of bots is known as a botnet. With a command to that channel, the hacker can use these bots to launch Denial of Service attacks against servers: sometimes, hundreds or thousands of bots all sending data to a server until its connection becomes saturated and/or the server crashes. Because the bots are making many computers attack from all over the world, this is called a Distributed Denial of Service attack (DDoS).

You can help stop the problem, not just by ensuring you don't get a trojan yourself, but by keeping alert for botnets and reporting them to network administrators. Recognizing a bot is not always easy, but there are some clues to look for. Check the nicknames. Sometimes the fake IRC "users" will have some part of their nicknames all in common (e.g., XY-lucy, XY-jane, XY-laura). With others, the nicknames look real, but nobody in the channel is chatting. Sometimes all of the nicknames, hosts, and real names look random (e.g., nickname =zjral, host = xcdv@isp.com, real name = rxfk).

When you do find them, what do you do? Report anything you think may be a botnet to an IRC administrator or other network administrator who can remove them from the network. UF users can report suspected botnet activity to abuse@ufl.edu [mailto:abuse@ufl.edu]. The best thing users can do is to protect their computers by following the rules about viruses, and
keeping all anti-virus software up to date.

For more information, see http://net-services.ufl.edu/security/public/worm-alert.shtml.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>