Published on *Tux Machines* (http://www.tuxmachines.org)

Computer viruses become hacker informants

By *srlinuxx*
Created *09/06/2005 - 2:39pm*
Submitted by srlinuxx on Thursday 9th of June 2005 02:39:48 PM Filed under Security [1]

An emerging breed of computer virus that keeps hackers informed about the latest weaknesses in computer networks has been discovered by security experts.

The viruses infect a computer network, scan for security vulnerabilities and then report back to hackers through an internet chatroom.

Armies of computers infected with "bot" viruses are routinely controlled via a chatroom connection. Typically these machines are used to knock a website offline with a "denial of service attack" or as a conduit for sending out spam email.

However, the ability of some bots to scan their hosts for unpatched security holes and report their findings back to hackers has gone largely unnoticed until now.

The emerging class of malware or malicious software - known as vulnerability assessment worms - "phone home" to allow hackers to fine-tune further attacks or perhaps even target an individual PC within a network.

This pernicious form of program is just one of a growing number of new viruses identified each month, says computer security expert Bruce Schneier.

"The virus trend doesn't look good," Schneier writes in the June 2005 edition of the Association for Computing Machinery journal, Queue. "More than a thousand new worms and viruses were discovered in the last six months alone."

Schneier cites the worm SpyBot.KEG, discovered in February 2005, as one of those in the vanguard of the vulnerability assessment worms. It reports the nature of vulnerabilities back to its author via an Internet Relay Chat (IRC) channel - a type of online chatroom.

Schneier expects newer IRC worms to emerge with even more complex vulnerability-exploiting behaviours. And he expects to see peer-to-peer file-trading networks becoming a major launch pad for new viruses.

Schneier's firm, California-based Counterpane Internet Security, monitors more than 400 corporate networks around the world and defends these against attack.

Kevin Hogan, senior manager at Symantec's Security Response division in Dublin, Ireland, says that the volume of new viruses is so vast because the source code for many programs is posted online, allowing anyone to make their own

variant.

"As soon as a new vulnerability is apparent in a server, someone can modify a bot to exploit it," Hogan says. "So the bot tells the hacker which machines on a network are vulnerable and it can be ordered to attack a host PC or a whole set of hosts, turning them into spam relays perhaps, or harvesting credit card numbers from their hard drives."

Hogan says that good firewall defences will prevent hackers from communicating with bots. And he says IRC has proved the downfall of many a botnet operator. Once the genuine IP address of the IRC channel host is known, tracking the hacker is not too difficult. "IRC is how they work, but it's also the Achilles heel of the botnet," he says.

Source [2].

Security

Source URL: http://www.tuxmachines.org/node/1265

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.newscientist.com/article.ns?id=dn7500