Malicious Bots Threaten Network Security

David Geer

Viruses, worms, Trojan horses, and network intrusions are among the threats that security administrators worry about on a regular basis. However, there is a less familiar threat that many experts say could be just as dangerous: malicious bot software.

A bot is a program that operates automatically as an agent for a user or another program. Hackers forward bots to victims by a number of means, and the software automatically infects vulnerable computers. The bots then wait for commands from a hacker, who can manipulate them and the infected systems without the user's knowledge.

A hacker can install bots on multiple computers to set up *botnets* that they can use for massive distributed-denial-of-service (DDoS) attacks that overwhelm victimized systems' defenses.

Network-security experts identify and shut down botnets with 10 to 100 compromised hosts several times a day. Crackdowns on large botnets with 10,000 or more hosts are rarer, but they still occur weekly, said Johannes Ullrich, chief technology officer for the Internet Storm Center, which detects, analyzes, and disseminates information about Internet-related security problems. The center is part of the SANS Institute, a network-security research and education organization. "Security investigators have even found one botnet of 100,000 computers," Ullrich noted.

Botnets can also be used for mass spam mailings, installing key-logging software that can steal victims' passwords and data, and compromising computers to prepare them for infection by future viruses.

Bot software is already on many computers. "As a baseline, we track about 250,000 infected systems a day. New ones come on, old ones fall off. We see as many as 60,000 come on in a day," said Alfred Huger, Symantec Security Response's senior director of engineering.

"Botnets have been one of the big underreported problems in security," noted Bruce Hughes, director of malicious-code research for security consultancy Cybertrust.

BOTS ON THE ATTACK

The challenge for attackers is to determine how to place bots on victims' computers, select their bot's attack methods, write or find the appropriate bot software, and then install it on victims' machines. Figure 1 shows a typical bot-infection process.

Hackers either write the bot programs themselves or reuse or modify existing code, noted David Dittrich, information assurance researcher at the University of Washington.

Attackers either can use their own computers to send bots and commands to victims or can use a machine they have infected, which then acts as a proxy server. These proxy servers can make finding the hacker difficult for security investigators.

Installing bots on target machines

Hackers typically send their malicious bots to many computers at one time. The bots then automatically infect the machines that have the backdoors or other vulnerabilities that the software was written to exploit via virus, worm, or Trojan horse components.

Bots take advantage of system vulnerabilities such as software bugs, including those that enable buffer-overflow attacks, hacker-installed backdoors, and various memory-management problems that allow malicious code to infect a system.

E-mail attachments with mass-mailing worms can carry bots. In addition, hackers can send bots via Internet relay chat (IRC) file-transfer mechanisms or other means to victims' potentially vulnerable TCP/IP ports.

Moreover, attackers can hack Web sites and install bots that infect surfers' vulnerable browsers. For example, hackers can attack buffer-overflow vulnerabilities in Web servers, changing HTML pages' header and footer information to include scripts. Visiting browsers activate the scripts, which cause the browser to download a bot.

The growth in the number of homes with always-on, high-speed broadband Internet connections has enabled hackers to spread bots widely and quickly, according to David Perry, global director of education for antivirus-software vendor Trend Micro. The broadband connections make it easier for attackers to both install bots on victim computers and use them to send spam and launch DDoS attacks.

Published by the IEEE Computer Society

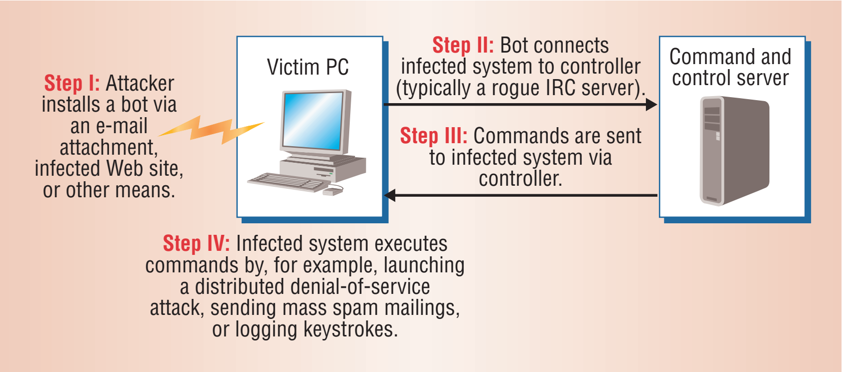
Step I: Attacker installs a bot via an e-mail attachment, infected Web site, or other means.
Victim PC
Step II: Bot connects infected system to controller (typically a rogue IRC server).
Command and control server
Step III: Commands are sent to infected system via controller.
Step IV: Infected system executes commands by, for example, launching a distributed denial-of-service attack, sending mass spam mailings, or logging keystrokes.

Figure 1. A typical bot attack.

Attack methods

Bots generally use one of several attack approaches, and quite a few can utilize multiple techniques. Some techniques are quite sophisticated. For example, Phatbot can generate new encryption for itself to look different to security software each time it infects a user. This makes it difficult for the software to find a common code signature for and thus recognize Phatbot, explained Joe Hartmann, Trend Micro's director for North American antivirus research.

Using such techniques, Phatbot has exploited multiple target-system vulnerabilities, infected many machines, and used brute force attacks on shared network resources to compromise networks, said Ken Dunham, director of malicious code for security consultancy iDefense.

Some attackers have even installed bots on multiple machines to create a distributed system that can be used for complex attacks, noted the University of Washington's Dittrich. For example, he said, such systems can launch distributed dictionary attacks to steal victims' passwords.

"It seems like a logical progression that people have added programmable [attack] mechanisms to the bots to add functionality," he said.

Chat. Most bots—including those in the large Phatbot/Agobot and Sdbot/Rbot families—use IRC as a way to communicate with and receive commands from hackers. However, many of these bots—which have tiny, built-in IRC clients—can also use other attack methods.

IRC has built-in multicast capabilities, which lets attackers quickly and easily send commands to all parts of a botnet. IRC thus lets hackers work with multicast capabilities without writing new code for the bot, noted Ed Skoudis, SANS instructor and consultant with Intelguardians, an IT security provider.

Peer-to-peer. Many bots, including some that can also work with IRC, are able to use peer-to-peer communications. These bots include P2P clients.

They connect to a server that uses Gnutella, an open-source file-sharing technology, and work with the WASTE file-sharing protocol. Rather than use a directory on a central server, WASTE has a distributed directory, which lets bots easily find and communicate with one another.

They can thus exchange hacker commands or other attack-related information among themselves. An attacker can initiate the process by serving as a peer in a P2P network and sending commands to one bot, which can then pass them on to the others.

Thus, hackers don't have to communicate with bots via IRC multicasting. Decentralized P2P-based bot systems are harder for security officials to trace or shut down than systems using a single IRC source.

If security officials discover and disable some of the bots in a sophisticated P2P system, Skoudis said, the bots can communicate this to one another and the attacker and then start spreading again to compensate for the losses. Each bot carries the software necessary to create and spread more bots.

Botnets. Hackers can install bots on multiple computers simultaneously—via such methods as e-mail attachments or IRC multicasts—to form a network. The bots can then act in unison via hackers' commands.

In a botnet, bots can communicate with one another or the hacker via IRC or P2P. Attackers can also set up an interface on infected machines and use it to remotely send commands to the computers. Hackers can also program bots to contact a Web server, which they set up to issue attack commands, said Skoudis.

"In one sense, botnets are a more dangerous problem than worms and viruses," the Internet Storm Center's Ullrich said, "They're an easy way to control 10,000 systems."

Hackers have used botnets to distribute large quantities of spam, noted Fred Cohen, managing director of the Fred Cohen & Associates security consultancy. Hackers can also use botnets to launch DDoS attacks by sending large numbers of messages to a target system.

Hackers generally used the early botnets for such attacks but now usually use them to send spam, noted Eugene Spafford, professor and executive director of Purdue University's Center for Education and Research in Information Assurance and Security.

Some bots can install keystroke loggers on victims' machines and capture passwords, credit card numbers, financial records, and other private information, added Rob Murawski, a technical staff member with the CERT Coordination Center, an Internet-security organization. The bots send the logged keystrokes back to hackers via e-mail or a Web server.

According to the UK's London Metropolitan Police (also known as Scotland Yard), "Small groups of young people creating a resource out of a 10,000- to 30,000-computer network are renting them out to anybody who has the money." Most of the people who control the rental botnets are from Eastern Europe.

"A typical botnet might go for as little as $20," said Trend Micro's Perry.

Hybrid threats. Hackers can write worms into bot software to create hybrid threats. Bots don't replicate or spread on their own, but they can use the worms' functionality to do so. In fact, hackers can spread bots more quickly with worms than with other methods. In addition, botnets can spread worms faster than worms can spread on their own.

Symantec's Security Response Team said 2004's Witty worm, which infected and crashed tens of thousands of servers, was probably launched by a botnet, according to Huger.

"We saw Witty break out more or less at the same time from 100 or more machines. The machines were all over the world, but they had something in common: They were on our bot list [of] compromised computers," he noted.

Bots and spam. "The preferred method of spamming is now via botnets," said Mark Sunner, chief technology officer at security company MessageLabs.

This is because botnets can send out large volumes of unsolicited e-mail and also hide the senders' identity, explained Trend Micro's Hartmann. Spam sent by botnets looks like it came from the infected computers, not the hacker's computer.

Bots let spammers send unsolicited e-mail via small SMTP servers they install on victims' computers.

Several recent high-profile viruses, including Sobig and MyDoom, infected computers with bots that helped spread spam.

Upgrading bots to attack new system vulnerabilities

With bots' source code commonly available online, hackers can quickly update the software to take advantage of new target-system vulnerabilities. Agobot, the most common bot family, lets hackers easily plug in new functionality, explained Symantec's Huger.

For example, hackers have upgraded Agobot to breach security through the Local Security Authority Subsystem Service vulnerability. LSASS, installed on most Windows systems during the past five years, validates local user PC logons but its vulnerabilities enable buffer overflows. Hackers have used the Agobot variant primarily for forwarding spam, according to Trend Micro's Perry.

Symantec's observation of Internet traffic reveals a growing number of computers infected by this Agobot variant, according to Huger. Although patches for the LSASS vulnerabilities are available, many users haven't downloaded them.

Malicious bots could be as dangerous as viruses, worms, and Trojan horses.

Hackers can also infect target systems with a Trojan horse programmed to download, from an FTP site or Web server, updated or new bot software.

Bot software is harder for security systems to detect than, for example, worm programs. Worms spread automatically and randomly, frequently creating large amounts of data traffic that network-monitoring security devices can pick up.

On the other hand, said Perry, hackers generally use only one computer to spread their bots and thus have the bandwidth to search only smaller networks for vulnerable systems to infect, thereby generating smaller amounts of traffic.

Also, bots are starting to run across TCP/IP port 80, designated for HTTP-based Web traffic. These bots look like regular Web traffic and thus are difficult for security systems to recognize as malicious code.

Moreover, the Internet Storm Center's Ullrich noted, "We are already seeing bot developers rapidly including more advanced exploit and detection-evasion techniques."

In addition, the University of Washington's Dittrich said, advances in technologies such as wireless communications will increase the number of devices, systems, and network types that bots can take over and use as bases for attacks.

However, Intelguardians' Skoudis explained, malicious-code-detection technologies are also improving and becoming more adaptable. Techniques that detect malicious applications based on their behavior—such as scanning a network for vulnerable systems—rather than on code signatures that could easily change will be better able to recognize and stop harmful bots.

Nonetheless, iDefense's Dunham said, improvements by hackers in ways to foil bot detection could hurt these countermeasures.

"In 2003, there were only 750 [malicious] bots reported. In 2004, there have already been over 2,300. There is a potential for a 400 percent increase in 2004 and 2005 over what we have seen. If that's the case, we could see up to 12,000 variants of bots appear in 2005," said Dunham.

"If we look at malicious software in general, we have seen a transition occur from individuals trying to develop bragging rights to malicious software written for financial gain or criminal enterprise," Purdue's Spafford said. "And the power of using the network against itself, which is possible by using botnets, is growing as the Internet grows." ■

David Geer is a freelance technology writer based in Ashtabula, Ohio. Contact him at geercom@alltel.net.

Editor: Lee Garber, *Computer*, l.garber@computer.org