IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2004 Published by the IEEE Computer Society
Vol. 5, No. 6; June 2004

Features Editor: Rebecca Deuel

Bot Software Spreads, Causes New Worries

Laurianne McLaughlin

Zombies attack! Bot software sounds a bit like a low-budget horror movie, but it's quietly making trouble and stealing data right now, using millions of PCs worldwide. These malicious pieces of code, often compared to an undercover army of robots, invade a PC and use its computing power to do someone else's dirty work—most often without the PC owner's knowledge.

The infected PC, known as a zombie, becomes another node on a bot network, typically 2,000 to 10,000 PCs strong, according to Symantec. Unfortunately, a bot network proves a practical tool for people who want to spread PC viruses and worms, send spam emails, install spyware on PCs, or carry out denial-of-service attacks on particular Web sites.

Technology publications have been buzzing about the bot threat ever since a flavor called Agobot took a fast ride through the Internet in April, finding its way into PCs thanks to a Windows operating system vulnerability. Security experts warn that large networks of Agobot-infected PCs now sit at the ready, waiting for directions. Have the risks been overblown, or do bots deserve special scrutiny?

"The risk has been overblown *and* [bots] deserve special scrutiny," says Bruce Schneier, founder and chief technical officer of Counterpane Internet Security. "They deserve special scrutiny because their risks are different than normal risks. Bots are risky because they do what they do automatically, and lots of them can work in tandem. So the relatively minor damage they can do —spam, worms, and so on—becomes nasty because a lot of it happens."

ANATOMY OF A BOT

"Good bots" that work at Web sites perform tasks such as scouring airline ticket prices or alerting customers when a particular item's price drops. In terms of technology, these bots have little in common with malicious bots, or remote access Trojan horses, as they were originally named.

Debuting around the year 2000, bot software took virus spreading to a new level by entering a PC and letting someone remotely use that PC to help with the dirty work. But this year, bot networks' use seems to have escalated quickly.

Why have bots become such a popular technology? For starters, bots aren't too difficult to create, says Joe Hartmann, Trend Micro's North American antivirus research director. "You have teenagers out there writing malicious code, and it's not that hard," he says. "Someone publishes the source code for a bot and suddenly a lot more people are releasing it."

Take Agobot, for example. In late April, security watchers found that the Agobot code had been tweaked and improved to exploit a security vulnerability related to a part of the Windows OS called the Local Security Authority Subsystem Service. LSASS is present in machines that run Windows 2000, Windows XP, and Windows Server 2003. Agobot uses IRC (Internet Relay Channel) chat to send data to and from the infected PCs.

Microsoft responded to the LSASS issue, asking people to install a security update (http://www.microsoft.com/security/incident/pctdisable.asp) first offered in early April that addressed about 20 Windows flaws that could result in virus or worm problems. But the LSASS route of attack worked on thousands of PCs. Consider the results for one month. In May, the most common Agobot strain was cleaned from 13,404 PCs using TrendMicro's Housecall service (http://housecall.antivirus.com; a free way to check a PC's health). In total that month, 50,204 systems were cleaned of some variety of Agobot. These figures don't include TrendMicro's corporate customers or PC-cillin product users, only people who used the online checkup service.

About 60 percent of the infections were from North America—notable, Hartmann says, because it points to how many US computer users still don't regularly run antivirus software. In May, TrendMicro saw between five and 10 new strains of Agobot every day, Hartmann says.

These modified versions of Agobot continue to pop up, as Agobot has proven itself an effective choice for creating a bot network. "It's not software development in the commercial sense of the word," says Alfred Huger, senior director of Symantec's Security Response team. "But people are building and selling frameworks for the bots." Online, people working with bots can now buy plug-and-play code for dropping in various exploits, he says.

The well-publicized Sasser worm used the same LSASS vulnerability that Agobot used, but Agobot will leave more lasting damage than Sasser because it leaves a trail of unaware PC owners who will continue to be victimized. This is a key difference between bots and worms, although people often use bots to lay the groundwork for forthcoming worms.

"A huge amount of press comes out with a worm," Huger says. "They're noisier than bots. [Worms] consume a huge amount of system resources, reboot PCs." So people are more likely to notice worms' effects on PCs and networks.

'MILLIONS' OF INFECTED PCS

It's hard to determine the precise size of the bot problem. According to Symantec, which measures bot activity as a 14-day moving average, 800,000 to 900,000 PCs at any given time are zombies infected with some type of bot. "The number is much larger, but those are the ones where we have empirical evidence," Huger says. The real number? "Certainly in the millions," he says.

The bot networks that Symantec discovers run anywhere from 40 systems to 400,000, Huger says, but average 2,000 to 10,000 hosts. The largest he's seen is a 400,000-host strong Phatbot network. Phatbot, an Agobot variant, uses an encrypted peer-to-peer network to talk to and use infected PCs.

Many of the infected PCs will have several varieties of bots and worms because one bot opens a back door and then another bot uses it. "Almost always, you see more than one bot residing on a system," Huger says.

A key problem: There's no easy way to reach owners of zombie PCs. Although Symantec contacts ISPs to alert them of large bot networks, it's up to the ISP to do something about it. Even if you learn that your PC has a bot, it's hard to eliminate all the back doors without wiping your system.

That means bot software has longevity. "We have seen hosts that have been infected for two years," Huger says. Bots continue to spread even elderly worms such as the Code Red worm, which is more than two years old. Symantec still sees 20,000 instances of the Code Red worm a day, Huger says.

Bot authors haven't bothered with Apple or Linux operating systems. "There's no reason to move on [from Windows]," Huger says. Windows offers the largest computing community and thus the largest target.

Other than educating and encouraging PC users to run antivirus and firewall software and keep up with operating system patches, the antivirus community can't do a whole lot at this point to stop bots that exploit Windows vulnerabilities.

Windows OS patches have become an unwelcome but routine part of life for many computer users. Some people in the computing community, such as Counterpane's Schneier, say one solution is to hold software vendors liable in certain cases of product glitches.

BIGGEST WORRIES

The worries related to bots range from small-time scams to large-scale network disruption. A bot network makes an affordable and well-disguised spam email factory. "There's a phenomenal volume taking place," Huger says. "That's the majority of the traffic that we see related to bots—probably 90 percent."

Bot networks can also be used for denial-of-service attacks on specific Internet domains. Symantec sees dozens of these each day. Down the road, identity theft might also become a real concern related to bots, which can be programmed to grab different types of data from infected PCs, says Trend Micro's Hartmann.

What worries Huger the most, however, is a bot's ability to preseed a worm that's more than simply mischievous and one for which no fix is readily available. "If someone used a preseeded network for a worm that was destructive, we'd be in for a really large problem," he says.

Consider, he says, how a bot network could help spread a so-called Warhol worm—one that infects the Net in record time, maybe an hour or two, for 15 minutes of fame for the author. While that scenario would worry anyone, small, less flashy crimes have been a mainstay for online crooks. Email scams work because they have to succeed with only a few people to make money for the scam's creators.

Bots make this type of activity even more attractive. "What worries me the most is that [bots] make marginal attacks profitable," Schneier says. Bots take automation to a new level.

NEW CRIMINALS, NEW REALITIES

Indeed, the environment for viruses, worms, and other malicious code now looks different, as Trend Micro warned in April. The company's TrendLabs division, which tracks malware activity worldwide, reported that about 60 percent of the new malware discovered in April involved backdoors. "This increase in backdoor programs illustrates an evolution in the objective of virus writers," according to a report by David Kopp, head of TrendLabs, EMEA.

Although many viruses of old seemed to be mostly about fame for the author, the backdoor programs such as bots could also be used for money. For example, bots can install key loggers and grab credit card information or email addresses—information authors can market in database form to less-than-reputable people online, Kopp says.

But are bots and other remote access programs the way of the future for online data theft and spreading bad code? Unfortunately, many security professionals say yes. "It's here, and it's here to stay," Symantec's Huger says. Compared to previous techniques used to distribute trouble online, "a bot network is exponentially faster."

CONCLUSION

Schneier sums up the problem. "There is a huge potential problem, because those bots represent a huge sleeper army that could be woken up and used for ill."

Related Links

Purchase or Digital Library members log in:

- **Botnets: Big and Bigger**, *IEEE Security & Privacy* (July/Aug. 2003)
  http://csdl.computer.org/comp/mags/sp/2003/04/j4087abs.htm

- **Automated Identity Theft**, *IEEE Security & Privacy* (Sept./Oct. 2003)
  http://csdl.computer.org/comp/mags/sp/2003/05/j5089abs.htm