Fast-Moving Zombies

Botnets Stay a Step Ahead of the Fixes

Greg Goth

The recent surge in broadband connectivity among the Internet’s residential users undoubtedly brings tremendous economic opportunity. However, not all that opportunity is driven by benevolent motives. Malware authors have discovered a bonanza in always-on connections that often feature vulnerable operating systems and feckless computer owners. Virus propagation, spam, click fraud, phishing, and other black hat activities boomed through botnets in 2006, and industry experts say the crisis has just started.

“The nature of threat has changed,” says Dan Druker, executive vice president of marketing at Postini, which offers email and messaging filtering and security services to 36,000 businesses globally. “2006 was the year botnets exploded and turned the market on its head. In the old days, attacks were done by some guy sitting in his basement who was paying for his own connection. Now I think of it as grid computing gone bad — they have infinite free computer power and free bandwidth. There is no way to stop this problem if you’re trying to do it yourself. Your costs will scale with the amount of attacks you’re receiving.”

Indeed, Druker says Postini has gleansed some distressing statistics: spam constituted 94 percent of all emails it studied in December 2006, and the company blocked more than 25 billion spam emails that month, a 144 percent increase from the previous December. However, the rapid expansion of botnet attacks might have a silver lining, according to several network security experts.

“I think this is really going to be the big year for much wider botnet awareness, much in the way 1995 and 1996 were big years for spam becoming part of the public’s knowledge,” says Paul Moriarty, Trend Micro’s product development director. “The technical community was aware of what spam could do back then, but the average Joe had no clue. I’m really hoping that happens for botnets. We’re seeing quite a surge in general and trade-press articles on botnets, and as the general press picks it up, we get better mindshare.”

Unfortunately, even if average users know what botnets do to their computers — and to the Internet at large — that might not do much to stem the problem, so vendors and academic researchers are stepping up their efforts to learn how botnets propagate and morph. However, as long as typical users remain ignorant of what experts call the “commonsense things” that keep their computers uninfected, it’s likely malware authors will continue to exploit those gaping security holes.

A Port in Every Home?

Users who might be truly interested in discovering whether their computers have been turned into bots can do a fairly simple check from the command prompt. Typing `netstat -an` reveals both local and foreign IP addresses and the port numbers via which they’ve communicated during the computer’s current session. Users who don’t use Internet Relay Chat (IRC) and see port 6667 displayed on the list of addresses in the command prompt can almost guarantee that their machines have been hijacked. However, many of the most vulnerable users probably aren’t capable of even calling up a command prompt, let alone scanning their connection for likely bot activity, and botmasters are getting more ingenious at hiding their tracks.

Trend Micro’s Moriarty says IRC is still a bot boulevard, but other protocols are now being exploited as well. “IRC is still predominantly the main source of communication,” Moriarty says. “However, starting around April and May of last year, we started noticing bots starting to use port 80. So now they’re blending in with the normal mix of Web traffic, and it gets a little more difficult to separate the wheat from the chaff.”

Another industry veteran also says he sees a trend away from IRC bots. Andre M. DiMino, cofounder of the Shadowserver Foundation (www.shadowserver.org), a volunteer-run resource center focusing on malware, botnets, and electronic fraud activity, says P2P botnets are making a strong appearance. “It’s definitely shifting,” DiMino says. “There’s a lot of P2P bot traffic now. For instance, the Nugache worm [discovered in late April 2006] was a real classic P2P worm. We now believe it was originally released as a proof-of-concept on [the normally unassigned] port 8 because we’re seeing more variants. Originally, it was really easy to find — it had a hard-coded list of IPs and was kind of dumb when we first

The author of the document is Greg Goth.
The Internet Society has established the ISOC Fellowship to the IETF, which it will present to technologists from developing countries to fund their IETF meeting attendance. Up to five people will be awarded fellowships for each IETF meeting. The program currently receives corporate sponsorship from Google; ISOC is also seeking additional sponsors.

More information on application and sponsorship opportunities is available at www.isoc.org/educpillar/fellowship.

The International Telecommunications Union and the GSM Association have signed a memorandum of understanding (MoU) focused on encouraging development of information and communication technology infrastructure in developing countries. The MoU — signed during the February meeting of the Global Symposium for Regulators in Dubai — focuses on government and industry collaboration, supporting projects for low-cost ICT access in underserved areas, and global industry benchmarking.


The European Commission has opened a consultation on proposed changes to European contract law aimed at making Internet commerce easier, more efficient, and more reliable. The proposed changes will affect eight EU Directives, including those on unfair contract terms, the sale of consumer goods, distance sales, doorstep sales, package travel, price indication, and timeshares.


Mozilla has released Gran Paradiso Alpha 2, reaching another milestone in its Firefox 3.0 development effort (code-named Gran Paradiso). The new Firefox version is being built on Gecko 1.9, Mozilla’s next-generation layout engine. Developers can use Gran Paradiso Alpha 2 to test several new Gecko 1.9 Alpha 2 features, including rewritten core layout code that affects width calculations for tables, floats, and absolutely positioned elements. Gran Paradiso Alpha 2 is available for Web application developers for testing purposes only.


In advance of its competition to develop new cryptographic hash algorithms to augment and revise federal information-processing standard (FIPS) 180-2, the US National Institute of Standards and Technology (NIST) has published a draft of its minimum candidate requirements and algorithm evaluation criteria. Submissions to revise FIPS 180-2 — which specifies several versions of the Secure Hash Algorithm — are due in late 2008.

NIST plans to choose a final standard by the end of 2011. The institute held an international competition for an Advanced Encryption Standard 10 years ago, selecting Rijndael following four years of analysis.

More information is available at www.nist.gov/hash-function.

The Open Geospatial Consortium has joined the W3C and is participating in Geospatial XG, a W3C incubator activity focusing on semantic geospatial issues. The activity’s goal is to develop a W3C note based on GeoRSS version 1 that will describe GeoRSS in the context of W3C standards such as XML, HTML, and OWL, as well as OGC’s Abstract Specification and Geography Markup Language.

More information is available at www.w3.org/2005/Incubator/geo.

Motorola, the GSM Association, and MTC Namibia have signed an agreement to conduct the world’s first trial of customer-based solar- and wind-powered systems to support GSM cell sites. The trials are scheduled to begin April 2007 and run through July 2007. The systems will power a remote cell site, which will carry its standard traffic level and remain a part of MTC Namibia’s wireless network.

One common vector DiMino and Moriarty highlight isn’t a network element, but rather that malware authors continue to poke around for Windows vulnerabilities. And, as the two attest, the old problem of balancing user convenience and network security is often vexing, leading to insecure lowest-common-denominator default settings and a seeming lack of focus in establishing a universal secure consumer configuration.

“In trying to focus the effort, one thing that would discourage the bad guys would be for home users not to run their machines with administrator privileges, but that’s difficult under the current configuration of XP,” DiMino says. “We hope Vista will do a better job. And egress filtering at any point is important.”

However, just as it might be hard to imagine home users typing in command prompts, egress filtering is also a potential minefield for the last-mile machines most likely to become bots. For example, whereas XP Service Pack 2 has no easily discernible way for users to configure their machines to avoid outgoing IRC communications, some ISP home network equipment does. AT&T’s broadband wireless router manufactured by 2Wire, for instance, lets users disable outgoing IRC traffic, but it’s not the default setting. And some users have been frustrated by system crashes caused by downloading other free firewalls that are incompatible with their ISP-supplied software, XP firewall, or both.

White Hats Rally

With the botnet threat growing more visible, so too are security experts’ reactions. Commercial and academic researchers have been writing and releasing more white papers on vari-
ous aspects of botnet propagation. A team of researchers from Georgia Tech University and the University of Central Florida has released papers relating to both botnet taxonomy (www.math.tulane.edu/~tcsem/botnets/ndss_botax.pdf) and modeling botnet propagation using time zones (www.isoc.org/isoc/conferences/ndss/06/proceedings/html/2006/papers/modeling_botnet_propagation.pdf). By employing epidemiological models of malware propagation, the authors claim, security experts and network operators can calculate likely peak times for malware authors to unleash botnets and thus prioritize resources for combating botnets in different time zones.

Although the security and research community has been sounding the warning about botnets, the ISP community hasn’t responded in kind, according to DiMino, Moriarty, and Druker. They say numerous factors contribute to this dilemma.

"Unfortunately, the best place to attack this problem is at the ISP, and it’s a very low-margin commodity business these days," Moriarty says. "At worst, you have to be cost-neutral going in. Most ISPs today will tell you, ‘If this is going to increase my call center volume, I don’t know if it’s worth it.’"

Perhaps part of the issue in getting ISPs to become more active in working with botnet researchers and vendors is that there is no perceived overall capacity crisis right now. If consumers’ basic broadband connections are running at 256 to 384 Kbps each way, for example, and communication to and from a bot herder is using far less of that than users perceive as a problem, they won’t complain—and the traffic moves on as usual.

"The problem is, we’ve discussed this with ISPs, and they put everything in monetary terms," DiMino says. "Right now, botnets don’t cost them enough per user to make them take action overall because they have the average time online per user figured out and it’s not a detriment so far. At some point, we’ve got to make them aware that ignoring the problem will cost them."

Druker says Postini’s clients are concerned with keeping their own networks up and running, and aren’t taking botnets’ wider implications into consideration. “Our charter is simply to make the problem go away for our client,” Druker says. “We’re not trying to disrupt the bad guys.”

If those behind botnets continue to use the most sophisticated methods of luring users to their ends, however, those data rates might become a concern.

“The main thing that had tremendous impact on email was the change from text-based messages to images and documents,” Druker says. “Images are quite a bit larger, and this drove the total amount of traffic up by 334 percent last year. There’s no threat to Internet infrastructure yet, but a tremendous threat to email infrastructure.”

This threat could, of course, creep into the network architecture at large, and vendors are moving rapidly to offer solutions. Trend Micro recently released its bot solution, called InterCloud Security Service, and Moriarty says the company has revisited its marketing strategy.

“There are a number of different techniques that can be used to detect botnet activity. Where it becomes tricky is the remediation piece. All you’re doing is creating a problem for an ISP if you’re just doing identification,” he says. “We, as an industry, haven’t done a really good job of providing ISPs to date with something they can use in an automatic way that doesn’t increase their call volume, which is one of their biggest costs.”

Ultimately, Moriarty says, the bot threat will probably be compared to the old door-lock analogy. “How far are you going to go, is what it boils down to. You can put an average lock on a door or install a stainless steel door with multiple deadbolts. It’ll be more secure, but probably overkill.”

Greg Goth is a freelance technology writer based in Connecticut.