



Bots of change

Escalating threats, smarter viruses, sneakier spam. Reading Symantec's Internet security threat report, a half-yearly publication which I've followed for many moons now, can be a pretty depressing exercise.

Still, dismal findings aside, these stats-laden reports often harbor interesting snippets of information that sometimes foretell new attack trends. And in the latest issue of Symantec's Asia Pacific and Japan Internet security threat report—which tallied results the security firm collected from July to December 2006—two findings piqued my interest.

Both have to do with bots—automated programs covertly installed in PCs as agents of crime by their human masters. Able to receive and act on instructions via communication channels like IRC, bots can be used to carry out a variety of malicious activities. For added impact, they do so in packs, syncing their efforts with similarly commandeered bots residing in other 'zombie' PCs.

The first Symantec finding has to do with the changing behavior of bots.

The security firm counted 2.2 million bot-infected machines in Asia Pacific as of December 2006, a tally that doubled the figures from six-month prior. No big surprise there.

What's surprising though, is that the number of denial of service (DoS) attacks actually dropped by five percent over the same period.

Now, DoS attacks have long been the main attack charter of bots. So for a rise in the number of bot-hosts to not induce a corresponding increase in DoS attacks can only mean that a fundamental behavioral change in botnet masters is afoot.

Symantec surmised that the results showed that attackers are changing the way they are using bots, to other more consistently profitable assignments such as relaying spam. One can also deduce that more bots are now being harnessed for covert ops like information theft, via traffic sniffing, key logging and other techniques.

In other words, bots are getting even more insidious.

The second finding concerned the worsening bot-infection trend in China.

According to Symantec, the world's most populous country harbored, as of last December, 26% of the six million bot-infected machines worldwide—a 29% increase from its previous six-month tally of 20% of 4.7 million bot-infected machines.

This it pointed the finger at China's dizzying broadband uptake rate. With new broadband users typically less security-minded, botnet masters would find China a rich hunting ground for machines to enslave, concluded Symantec.

According to internetworldstats.com, China now accounted for 11% of global broadband users and will surpass the U.S. on that count next year. According to market researcher Ovum, China's broadband market will grow by a CAGR of 75% to reach 139 million subscribers by 2010.

Expect, therefore, a prolonging of the worsening bot trend in China.

But don't expect a deluge of news about botnets being uncovered by end-users and organizations anytime soon because, as Symantec Singapore's senior consultant Ooi

Szu-Khiam pointed out, bots are getting harder to detect despite being more widespread. Also, botnet masters aren't likely to engage in big-bang attacks these days. "You can be sure they aren't going to take down Websites like Yahoo," he said.

He noted too that newer bots have begun to use rootkit techniques to mask their presence. This could mean, he said, that thwarting bots in the future may increasingly

require non-conventional scanners that can detect operating system kernel-level anomalies.

For now, said Ooi, the best defense for the individual user is still the triumvirate of antivirus, firewall and regular up-to-date patches.

As for people who manage IT systems and network security, Judhi Prasetyo, country manager, Singapore & Emerging Markets, Fortinet offered two further tips.

The first is to keep a keen eye on network statistics and events, especially watching out for unusual URLs, IP addresses and ports that user computers may be going to. Pay attention to unexpected spikes in network activities or dips in system performance, he said. Both are harbingers to bot-related activities like DDoS and mass spamming.

System administrators should also keep a tight-fisted control on network ports, said Prasetyo. "Open only those network ports that are absolutely necessary for the known services on your network," he said. Shutter everything else. In the battle with bots, don't give them a headstart by opening unnecessary doors. NWA

**Expect, therefore,
a prolonging of the
worsening bot trend in
China.**

Ong Boon Kiat Editor boonkiat@questexasia.com