

Press Release

Are bots about to bring down your business?

London, UK - June 10, 2008 - There's some good news these days on the IT security front: Cybercriminals don't want to knock your network offline. The bad news? They want to use it for launching attacks that are more distributed, more profitable and potentially more damaging to your business than ever before.

Cybercriminals need enterprise systems to maximise the effectiveness of bots—the rogue, hard-to-detect programs they use to seize computers and rope them into larger collections of similarly compromised machines known as botnets. And they have far more in mind than flooding servers or propagating worms: Botnets provide an efficient, distributed architecture for staging large-scale raids on information and blasting spam. As such, they're reflective of the evolution of cybercrime from mischievous hacking and malware-writing to well-organised schemes for stealing data on a global scale and selling it for maximum profit. Witness the bust in February 2008 of a 17-person Canadian ring running a one-million-computer botnet that led to nearly \$50 million in business losses.

Clearly, bots and botnets pose yet another threat to valuable corporate data. A potentially bigger worry: the as-yet undetermined liability of companies whose systems are unknowingly used in the theft of data or delivery of spam. What's more, any time that the security of confidential information is compromised, organisations run the risk of noncompliance with the numerous regulations now on the books—not to mention losing the trust of their customers and business partners. In short, bots and botnets may not necessarily lead to expensive downtime, but they could be a lot more costly to your company in other ways.

Fortunately, there are ways to defend against the threat of bots. As always, educating users is a great place to start, since bots usually download themselves from sites they shouldn't be visiting from work in the first place, or from e-mailed links they have no reason to click. A necessary corollary to that strategy: Update acceptable use policies, and make it clear that violators will face the consequences.

Of course, finding the right security technology is also essential in the fight against bots. Implementing a Web filtering solution that stops bots at the gateway—before they even have a chance to land on corporate systems—gives organizations the protection they need, and the assurance that bots won't spell the end of their business.

As IT professionals are aware, bots aren't bad by their nature. Also known as Web robots, crawlers, or spiders, they are, at their most basic, simple software scripts used to run automated tasks over the Internet. These include searching for content, posting messages to multiple newsgroups or sifting through data to make online comparison shopping possible.

As with all things online, however, bots can be used for less noble purposes. Ticket brokering agencies, for example, may deploy bots against entertainment or sporting event sites to gather up as many of the best seats possible for reselling at maximum profit. Participants in multiplayer, online role-playing games also have been known to use bots to seek and gather information for competitive advantage—information that would otherwise require too much time or effort to obtain.

But those endeavors are tame in comparison to the nefarious, large-scale operations in which cybercriminals now specialise. They know there's a lot of valuable information stored on employee and corporate systems, and they know that bots can help them get it. Once in possession of this data, they turn around and sell it to the highest bidder. This has helped turn an underground market for stolen and re-sold information into a global business involving tens of millions of dollars.

Bots can land on user systems by seemingly innocuous ways: via drive-by downloads from visits to unauthorised sites, by clicking on links in suspicious e-mail messages or even by mousing over compromised banner advertising. Bots are built to elude detection, morphing as they travel so that most anti-spyware, -spam, and -virus packages can't catch them; and by lying dormant on computers, without affecting performance or otherwise calling attention to themselves. If the opposite were true, cybercriminals would be robbed of the weapon that's truly vital to their mission: the user computer itself.

Any security vulnerability is potentially damaging to your business, and bots and botnets definitely fit the bill. When rogue programs are running on employee machines, companies are right to worry about the safety and integrity of their data and their systems, and whether compromised information and performance could affect not just their competitiveness—but their viability.

Defending your organization against bots and botnets is in many ways similar to warding off malware. Still, this threat poses particular changes so companies should consider the following comprehensive approach:

- Deploy security solutions like anti-virus and anti-spyware, which could help in stopping bots at the end-point
- Deploy gateway security solutions that can scan e-mail and Web traffic to prevent users from accidentally downloading bots. These solutions can also be used to detect outbound traffic from bots, helping identify bot-infected machines on the network
- Set up a proactive security response group, and assign them responsibility for dealing rapidly with infected machines, keeping patches current and the security infrastructure up to date
- Conduct frequent user training, educating employees on how to recognize e-mail and IM scams and avoid falling for the social engineering techniques used to propagate bots

As with all potential security threats, companies need to respond with a range of measures, including educating users on how to avoid downloading bots and creating a rapid-response team to deal with the dangers bots and botnets present. Also essential to the effort is a gateway security solution that can stop bots before they land on the network and that can detect outbound botnet traffic.

By George Shih, CEO 8e6 Technologies, ZDNet, News.com

Posted on ZDNet News: Jun 10, 2008 12:00:00 AM

About 8e6 Technologies

8e6 Technologies is the leading independent provider of Web filtering and insider threat management solutions for mid-size to large enterprises, protecting millions of users worldwide. The company's award-winning appliance suite requires no additional infrastructure or software to install, resulting in the lowest total cost of ownership on the market. 8e6 is recognized for its real-time analysis, reporting capabilities and unmatched forensics that reduce security, legal and compliance risk. The company's solutions are customizable to meet individual customer requirements, yet are powerful enough to meet the performance demands of the largest corporations in the world. A Web filtering pioneer since 1995, the company maintains headquarters in Orange, California, and has a network of channel partners worldwide. For more information, please call +1 888 786 7999 or visit www.8e6.com.

Contact

Eric Lundbohm
8e6 Technologies
+1 714 282 6111
elundbohm@8e6.com

Ed Barker or Luke Nava
Schwartz Communications
+44 (0) 20 7268 3028
8e6@schwartz-pr.com