

JIM RAPOZA

Botnets vs. botnets

Understand and use the tools of the enemies to catch them

WHEN IT COMES TO defending technology assets against malicious hackers and other bad guys, I've always been a firm believer in understanding and even using the tools and tactics of the enemy.

In most cases this means having familiarity and even a working knowledge of the tools and methods that are used to scan and compromise networks and systems. But I've also been in favor of more proactive means of protection, from the use of tarpits and honeypots to my advocacy of the use of good worms to seek out and patch systems with holes that could be exploited by attackers and malicious worms.

So it should be understandable that I was very interested in a paper that was presented at the recent USENIX Symposium. This paper, by several researchers at the University of Washington, advocates the creation and use of friendly botnets to slow and even stop the evil botnets that are used to attack and bring down Web sites and servers.

The idea is that it's possible to take a swarm of friendly computing systems—essentially a botnet but something that the paper calls a pha-

lanx—and place it in front of Web sites and servers. All communication with the site passes through this cluster of systems, and data is passed to the server only at the server's request.

Now, imagine an evil botnet attacks the site protected by the phalanx. Instead of the full network wave of the evil botnet crushing the server and bringing it down, most of the traffic would be stopped by the phalanx

phalanx botnets. The giant content delivery networks have vast amounts of computing resources at their disposal, so it would be relatively trivial to repurpose some of this for use as secure good botnets.

Also, there are plenty of examples of people voluntarily contributing computing resources to distributed causes, with the popular SETI@home as probably the best-known example. As the paper points



Tarpits, honeypots and good worms can be used to seek and patch holes.

systems, with only a small amount of traffic reaching the main server. Best of all, even under a massive denial of service attack, a server protected in this way will stay up and running.

But where will these good botnet systems originate? The bad guys use worms and rootkits to take over zombie systems and make them part of their botnets; will the good guys force systems to be part of their good phalanx botnets?

Actually, there are already plenty of computing resources available for use as good

out, it even could be possible to use things such as BitTorrent to build good phalanx botnets to stop the evil botnets.

Sure, security constantly changes and the bad guys will eventually come up with new tactics, but this phalanx idea looks to be a very good approach to protecting servers and Web sites.

Like the old saying it takes a thief to catch a thief, it may take a botnet to stop a botnet. ☛

Chief Technology Analyst Jim Rapoza can be reached at jrapoza@eweek.com.