darkREADING
RISKY BUSINESS

How to Root Out Bots in Your Network

Expert gives tips on how to detect and remediate internal botnet infestations

OCTOBER 2, 2008 | 5:40 PM

By Kelly Jackson Higgins
Senior Editor, *Dark Reading*

Even routinely clean antivirus scans can't hide the dirty little secret more enterprises are facing today: Some of their client machines are members of botnets.

That's why Matt Sergeant, senior anti-spam technologist for MessageLabs Ltd. , hopes to educate some large organizations and ISPs on how to detect and clean up their bot-infested machines next week at the SecTor security conference in Toronto. Sergeant says a little grass-roots help with botnet detection would help. "There aren't enough DNS blacklists tracking botnets. That's not good for the anti-spam economy," he says. "I would like to see more people tracking these things, listing IP addresses, and that type of thing."

Big organizations can start by cleaning up their own house. While the size and scope of the botnet problem continues to grow -- 90 percent of all spam comes from bots -- awareness of the botnet problem is still relatively low among enterprises, Sergeant says. Enterprises are often caught off guard when they realize they harbor bots; they assume antivirus engines will catch them, but they typically don't, he says. "So often we hear that they are running multiple AV and haven't found anything. But we're still seeing [bots there] when AV hasn't found them," Sergeant says.

Antivirus (AV) technology struggles when it comes to bot infections, he says, because AV vendors get tens of thousands of new pieces of malware samples every day, and there's simply no way they can keep up with that, he says. Botnets also tend to operate in multiple stages: A user may first get infected by a piece of malware, but by the time AV detects it, the malware will have downloaded a second stage of malware, deleting the original infected file, for instance, he says. Many botnets also disable AV so they can remain undetected, Sergeant says.

Sergeant says it takes a lot of determination and some expertise to detect bots in-house. "This type of thing is time-consuming. You have to be able to recognize patterns in large quantities of email, and recognize new things coming in," Sergeant says. And most mail servers don't provide the level of detail on messages that you need to weed out bot-borne messages.

The first step is to block Port 25 for both incoming and outgoing traffic -- except to your mail server, he says. Your firewall logs should reveal any client machines trying to spam out of your network. One hint: Bots tend to do more DNS queries than normal, so keep an eye on that as well as any MX lookups and .ru, .cn, and .info lookups, which are often red flags for bots trying to communicate with their command-and-control server.

Sergeant also recommends TCP fingerprinting, where you look for specific characteristics of known botnets -- Srizbi, for instance, has a custom TCP stack that you can look out for. You can merely watch for unusual volumes of bot traffic in your network, too, and track flow data, for instance. But before you go there, consult the legal department.

Sometimes, setting up honeypots to entrap botnet traffic, or darknets, is an option too, Sergeant says.

But performing your own bot investigations is like playing with fire, he warns. If the botnet recognizes that you're probing it, beware that it could turn on you very quickly. "The biggest risk is a denial-of-service (DOS) attack. With a number of botnets, if you try to probe them, and they recognize it's from a single IP address, they will turn around and attack your network. That's a high risk. I do not recommend any kind of probing unless you have a strong DOS [defense] in place," Sergeant says.

And remember that you're dealing with criminals, so there are potential consequences, he says. "Make sure

you have good lawyers."

So if you do find a bot in your network, then what? Clean the machine and then alert the upstream service provider to get the C&C machines shut down, he says. "You can take legal action, block completely any access to your firewall from that IP address range, or start up your own block-list system."

But don't expect any major support from law enforcement if you discover a big bot infestation. "The downside of all of this is law enforcement is really very weak on this," he says. "There's a huge gap in the enforcement."

Sergeant will present his research and tips in his "Tracking Current and Future Botnets" presentation on October 7 at SecTor.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading*'s editors directly, send us a message.*

- MessageLabs Ltd.