

## Defeating the Botnets of the Future

The following article is excerpted from *Understanding and Blocking the New Botnets*, a white paper researched and written by Scott Pinzon, CISSP, and Corey Nachreiner, CISSP, of the WatchGuard® LiveSecurity® team. For a fascinating look at botnets, how they evolved, and how they work today, download a free copy of the white paper at [www.watchguard.com/whitepapers.asp](http://www.watchguard.com/whitepapers.asp).

Botnets embody the ultimate blended threat. Botnet code carries almost every conceivable form of malware, from spyware to downloaders, rootkits, spam engines, and more. To answer like with like, defenders must employ multiple layers of security. The good news is that time-honored techniques are still surprisingly effective against botnets. Below we suggest countermeasures that greatly mitigate the likelihood of a bot infection operating from your network.

### 1. Patch promptly

Bots can draw upon a wide variety of exploits in order to infect victims. However, the biggest and most successful bots have relied upon exploiting vulnerabilities *that the vendor patched six to eighteen months earlier*. In the most extreme cases, we've seen bots attempting exploits against vulnerabilities that were patched as long as four years earlier. We can't account for why bot communications and back-end systems innovate at a breathtaking pace, while the bot uses exploits that are known and old. Our best guess is that botmasters find exploits by waiting for vendors to patch a vulnerability, then reverse-engineering the patch to find out what the flaw was.

We expect that exploiting more recent flaws will be one of the next areas for botmasters to improve upon. But for now, it is good news for the average network administrator. If you patch promptly when vendors release fixes for software you run on your network, you can move faster than the botmasters and resist their exploits.

### 2. Block JavaScript

When a bot leveraging web-based exploits attacks a victim computer, it invariably does so by executing JavaScript. Setting browsers to prompt before executing JavaScripts will eliminate a huge swath of bot infection vectors. We highly recommend having users rely on Firefox as their primary browser, using the [NoScript plug-in](#) to prompt whenever a script tries to execute.

### 3. Watch Those Ports

This is a two-part recommendation.

1) Even though the latest bots can communicate over ports every administrator must leave open, the vast majority of bots still communicate using IRC (port 6667) and other odd, high-numbered ports (such as 31337 and 54321). All ports above 1024 should be set to block both inbound and outbound unless your organization has a custom application or special need to open a given port. Even then, you can open a port carefully, implementing policies such as "open only during business hours" or "deny all, except traffic from the following list of trusted IP addresses." This simple measure prevents the garden variety and slow-adopter bots from reaching their Command and Control Center (C&C) for instructions and updates, essentially killing such bots on arrival.

2) Botnet traffic that travels over needed ports such as 80 or 7 often gives itself away by generating traffic when there should be none. Commonly, botmasters update their zombies between 1:00 a.m. and 5:00 a.m., when they assume no one is watching. Make a habit of checking your server logs in the morning. If you see web browsing activity when no one was there to do the browsing, that's your cue to investigate.

Administrators using WatchGuard Firebox® models will be pleased to know that the Firebox's proxies stop non-standard traffic attempting to run on standard ports. For example, the spamming botnet Mega-D runs non-standard, homebrew traffic over HTTP port 80. The Firebox's HTTP Proxy would spot and block such traffic instantly, by default.

#### 4. Redouble user awareness training

Some bots perform mass scans of the Internet, find vulnerable machines, and infect them. This practice is actually diminishing. More often now, bots "social engineer" their way onto your network by enticing a victim to click a link or open a file. These bots have the same restrictions as certain legendary vampires: they can't cross your threshold unless you invite them in.

This "luring" approach has gradually constricted itself even further. Attackers used to send malicious executable code as an attachment to an email. This practice has also fallen into the minority. Most of the action now is web-based. Malicious emails that would have contained an attachment two years ago now contain a link to a malicious site instead. Innocuous web sites can be infected by Mpack or other surreptitious malware to infect visitors who arrived by clicking recklessly.

That's your cue to explain to users, in terms they can understand, why they should never invite the vampire in. Tell them not to open attachments that arrive unsolicited and unexpected; why they shouldn't click links in email; and why they must think twice about any unusual links they click. If you need a starting point, try circulating our video that shows how drive-by downloads work, described for a non-technical audience: <http://video.google.com/videoplay?docid=-4094518401580008932>. Diligently applying controls such as those we have cited above have allowed networks to run free of bots for years.

#### 5. Stay vigilant

This recommendation seems too obvious to mention, almost like "Try not to get infected!" Yet we keep meeting IT administrators who spend so much time putting out fires and maintaining an understaffed help desk, they never look at their system logs. They never monitor bandwidth usage. They can't tell you who is connecting to what from their network. They have devices connected to their network that they don't even know about.

If this describes you, all we can say is, you are begging for trouble. You might even have bots on your network as you read this. If you are an administrator who rarely checks your logs, you must start reading them. Today. Once you learn what "normal" looks like on your network, 30 minutes a day is all you need for a spot check.

If this describes you, the odds are you are not lazy – you are constrained by lack of personnel and resources. Explain the threat to your bosses and see whether they'll support you in blocking out a half hour each morning for checking the status of your network. This time segment should be defended against meeting requests, conference calls, and other typical interruptions. This form of insurance is dirt cheap compared to the cost of a network compromise.

---

We believe the recent unprecedented bot breakthroughs merely foreshadow innovations to come. As never before in our years in Internet security, each month seems to bring newly discovered exploits *that researchers cannot fully explain*.

It turns out that botnets have been blended threats, but they have not been *ultimate* blended threats. Botmasters now freely supplement the traditional botnet architecture with added components that enhance automation, administration, and evasion. These combinations of technologies are frighteningly sophisticated and surprisingly polished. Any observer can safely predict that this trend will not only continue, but grow.

Are the bad guys winning? Obviously not, since we're still banking and buying over the Internet. But the flood of bot activity is rising, so we must push back, damming up the bot flood and revealing their masters' techniques. A simple way to undermine a botmaster's power is to make it difficult for bot code to recruit victims. WatchGuard security appliances use numerous layers of security, intelligently applied across many protocols, with powerful proxy technology that scrubs both inbound and outbound traffic to keep your network safe.

For information about WatchGuard security solutions and the protection they provide against botnets and other network threats, visit us at [www.watchguard.com](http://www.watchguard.com) or contact your reseller.

©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66528\_050608