

The Zotob Storm

If you'll forgive the possible comparison to hurricanes, Internet epidemics are much like severe weather: they happen randomly, they affect some segments of the population more than others, and your previous preparation determines how effective your defense is.



BRUCE SCHNEIER
Counterpane Internet Security

Zotob was the first major worm outbreak since MyDoom in January 2004. It happened quickly—less than five days after Microsoft published a critical security bulletin (its 39th of the year). Zotob's effects varied greatly from organization to organization: some networks were brought to their knees, while others didn't even notice.

The worm started spreading on Sunday, 14 August. Honestly, it wasn't much of a big deal, but it got a lot of play in the press because it hit several major news outlets, most notably CNN. If a news organization is personally affected by something, it's much more likely to report extensively on it. But my company, Counterpane Internet Security, monitors more than 500 networks worldwide, and we didn't think it was worth all the press coverage.

By the 17th, there were at least a dozen other worms that exploited the same vulnerability, both Zotob variants and others that were completely different. Most of them tried to recruit computers for bot networks, and some of the different variants warred against each other—stealing “owned” computers back and forth. If your network was infected, it was a mess.

Two weeks later, the 18-year-old who wrote the original Zotob worm was arrested, along with the 21-year-

old who paid him to write it. It seems likely the person who funded the worm's creation was not a hacker, but rather a criminal looking to profit.

The nature of worms has changed in the past few years. Previously, hackers looking for prestige or just wanting to cause damage were responsible for most worms. Today, they're increasingly written or commissioned by criminals. By taking over computers, worms can send spam, launch denial-of-service extortion attacks, or search for credit-card numbers and other personal information.

What could you have done beforehand to protect yourself against Zotob and its kin? “Install the patch” is the obvious answer, but it's not really a satisfactory one. There are simply too many patches. Although a single computer user can easily set up patches to automatically download and install—at least Microsoft Windows system patches—large corporate networks can't. Far too often, patches cause other things to break.

It would be great to know which patches are actually important and which ones just sound important. Before that weekend in August, the patch that would have protected against Zotob was just another patch; by Monday morning, it was the most important thing a sysadmin could do to secure the network.

Microsoft had six new patches available on 9 August, three designated as critical (including the one that Zotob used), one important, and two moderate. Could you have guessed beforehand which one would have actually been critical? With the next patch release, will you know which ones you can put off and for which ones you need to drop everything, test, and install across your network?

Given that it's impossible to know what's coming beforehand, how you respond to an actual worm largely determines your defense's effectiveness. You might need to respond quickly, and you most certainly need to respond accurately. Because it's impossible to know beforehand what the necessary response should be, you need a process for that response. Employees come and go, so the only thing that ensures a continuity of effective security is a process. You need accurate and timely information to fuel this process. And finally, you need experts to decipher the information, determine what to do, and implement a solution.

The Zotob storm was both typical and unique. It started soon after the vulnerability was published, but I don't think that made a difference. Even worms that use six-month-old vulnerabilities find huge swaths of the Internet unpatched. It was a surprise, but they all are. □

Bruce Schneier is one of the world's foremost security experts and chief technical officer of Counterpane Internet Security. His most recent book is Beyond Fear: Thinking Sensibly about Security in an Uncertain World. You can read his blog and subscribe to his newsletter, Cryptogram, at www.schneier.com.