

## ‘Genotyping’ Fends off Onslaught of Virus Variants

May 18, 2005

By Sharon Gaudin

**A**n IT administrator at the Maryland Department of the Environment no longer worries about the alphabet soup of virus families that used to plague his work day. Now he downloads one virus update and feels safe from the onslaught of variants that is likely to follow.

"Keeping up with the updates was a real chore," says Henry C. Torrance, the lead computer network specialist at the state agency, which has 1,200 users, eight offices and 30 to 35 servers. "I'm not worried about 10 patches a day. I'm just looking for one file that covers several different viruses in the same family. It covers the alphabet soup."

Torrance says the new genotyping technology from Sophos, Inc., an anti-virus and anti-spam company with U.S. headquarters based in Lynnfield, Mass., is slashing the time he has to allocate to dealing with virus updates.

Sophos started using this genotyping technology last summer, according to Marc Borbas, product manager for Gateway Solutions at Sophos. And since then, they have been quietly working it into a growing number of virus updates.

The genotype technology, according to Borbas, is designed to identify variants of a particular malware family. For instance, once a genotype update has been issued for Mydoom or Mytob, that one update is aimed at protecting against the army of variants that will follow the original worm or virus.

Borbas explains that genotyping looks

for certain genetic characteristics in one family. How does it interact with the operating system? Does it copy itself to a certain folder? Does it open a backdoor? Does it infect other files on your machine? Once these types of characteristics are noted, the technology will look for them in any variants that may follow the original malware, enabling the software to protect against the new worm or virus without a new virus update being sent out.

"With viruses, it's the variants that are becoming so hard to deal with," says Borbas. "When something new comes out, you have to get it in the lab and find out how to protect against it. That can take anywhere from an hour and a half to a day or two days... What the genotype does is add another layer of protection."

Borbas acknowledges that other companies have tried and are working on anti-virus software that detects behavior. Some of those have met with dismal results because of a high rate of false positives. He says the Sophos product is different because it looks for very specific traits.

"Mydoom had 50 or 60 variants," he says, adding that genotyping detected 77 percent of those variants from the single update. "That means if you're a corporate security manager sitting there fighting the Mydoom virus, 77 percent of the time you didn't have to do anything. Twenty-five percent of the time you did have to handle an update, but it was a substantial improvement."

Paul Stamp, an analyst at Forrester Research, an analyst firm based in Cambridge, Mass., says some anti-virus

companies have taken the approach where they look for a straight match. Other companies have looked for general behaviors. Few, if any, of those efforts worked.

Sophos' genotyping, however, combines those two methods, and has a more successful model, he says.

"This takes a layer of complexity out of the update process," says Stamp, who adds that he hasn't seen this technology elsewhere yet. "The less frequently you have to do [updates], the less complicated it is."

Sophos analysts are using the genotyping to both protect users against viruses but also to help filter out spam, which often uses similar email headers, key words and phrases, and patterns of html tags.

Andrew Jaquith, a senior analyst at the Boston-based analyst firm the Yankee Group, says fighting virus writers and spammers today is always a tricky business.

"Everybody is looking for more clever ways to get a leg up on the bad guys," he says. "It's an arms race. This represents an escalation on the defense. So good for them. But then the bad guys will escalate."

For today, anyway, Torrance says he has less updating to do and his users are happier — and that's a powerful combination for any IT shop.

"To be honest, I don't even worry about my anti-virus updating system," he adds. "That's how reliable it's been... We actually have end users now who have emailed us back saying, 'Thanks for choosing Sophos.' That's a pretty bizarre testimonial from end users who don't have any say in what product we choose."



Reprinted with permission INTERNET.COM, May 18, 2005.  
Copyright 2005 by Jupitermedia Corporation, <http://www.jupitermedia.com>. All rights reserved. For reorders, call 651-415-2300.

500927