In coming weeks, I will be reviewing the information security resources upon which I rely most often. In the first few issues of the new series, we have been looking at alerts and vulnerabilities.

Thanks to unschooled, naïve users who forward anything they receive without even _thinking_ about checking for correctness, network users often report false news to their colleagues on a network. As shown in the recent outbreak of the SULFNBK hoax (where messages convinced some people to delete a perfectly harmless and useful file out of fear that it carried a virus), hoaxes can convert gullible users into agents of destruction. In common with most other security specialists, I recommend that every organization explicitly ban distribution of warnings except through an authorized channel such as a network operations center, security team, technical support group or Help Desk.

The Hype or Hot page <http://www.trusecure.com/html/tspub/hypeorhot/index.shtml> at TruSecure Corporation (where I was Director of Education from 1991 to 1999) has useful information for network administrators trying to sort through the Internet babble of warnings about new malicious software. When I visited the page to write this article, the top news included a brief description of the W32/MsWorld@mm Trojan, which is described concisely as follows: “This appears to be a Shockwave movie compiled into an exe file. It purports to show pictures of Miss World beauty contestants, and in fact does show a few pictures, most of which have been morphed into mildly amusing caricatures.”

A real worm is VBS/BVSWG.Z@MM (also known as vbs/mawanella or vbs/nella.a@mm); it is described as follows: “This worm is hand-written (badly laid-out and untidy, but it works, and is spreading rapidly), and is modelled on standard vbswg kit generated ones. The point for the hand-rewriting is to achieve the displaying of the desired message. This isn't possible with pure kit-generated stuff. The message, by the way, is a political one to call attention to strife in Sri Lanka. As with other vbswg examples, it has no auto-start capability -- victims have double click the attachment to start it. It makes no special attempt to hide itself, and offers no startling new technology or twists, so it shouldn't get anywhere. Unfortunately, it is being reported from several countries around the world. As usual, anyone who is folowing TruSecure guidelines, and is filtering off .vbs attachments has little to fear.”

The site includes archives of previous analyses and has recently announced that the Hype or Hot page is now available via the AvantGo wireless service for hand-held devices. Even Internet-enabled cellular phones can reach the page by using the URL <http://www.trusecure.com/hdml/hoh/index.hdml>.

Congratulations to my long-standing friends and colleagues at TruSecure for this useful resource.

* * *
Finally, a quick word about the most comprehensive and well-run hoax site on the Internet, Rob Rosenbergers’s Vmyths.com <http://www.vmyths.com/>. In addition to an extensive and easily used search engine (just enter any key words you think might be specific to a message and you’ll get a list of possible hoaxes that use those words), the site features hard-hitting commentary from Rosenberger and his bebunking friends such as George C. Smith (author of the 1994 classic, _The Virus Creation Labs: A Journey into the Underground._ American Eagle Publications, Tucson, AZ, ISBN 0-929408-09-8; 172 pp). Some of the entertaining and though-provoking articles on the site when I visited it while researching this article:

Q&A: how often does virus hysteria occur? We coined the new term "hystericane" (a contraction of "hysteria hurricane"). These events follow a regular cycle, too. In other words, we can begin to predict hystericanes like sulfnbk.exe... [6/4/01]

Mumblings of monkey-men mock moderation: India's gov't may force its military to track down a mythical "monkey-man" beast. Well, what a coincidence! The U.S. gov't goes to great lengths to track down mythical electronic monkey-men... George C. Smith reports. [6/5/01]

sulfnbk.exe virus: It's not a hoax per se -- it's actually a mass-hysteria urban legend. Sadly, a bunch of clueless people keep rewriting the alert. Just one more reason why virus news should come directly from a virus expert... [5/29/01]

sulfnbk.exe food for thought: The sulfnbk.exe hysteria raised some wild philosophical questions. Vmyths.com has the intelligence (and the guts) to ask them... Rob Rosenberger reports. [6/4/01]

This site deserves an award for the exaltation of skepticism and common sense. It can be listed in every network security handbook as the first place to look for a quick take on whether a warning you get from a friend is bogus or not. If I heard on National Public Radio that a giant meteor were about to crash into our planet, I’d check vmyths.com before believing the report.

* * *

The next articles in this series will focus on security-awareness resources.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.