



Dispelling Viral Voodoo
infectionvectors.com
December 2004

Overview

The widespread fear and misunderstanding of computer viruses leads many people to blame a virus for any unexplained behavior. The viral “boogie man” takes the blame for all types of problems, many of which would require magic to accomplish with a virus. This brief report examines some of the reasons for the misunderstanding and the results of this confusion.

Tell Everyone You Know

Virus hoaxes are some of the most forwarded messages on the Internet. Hoaxes generally start with a story about how someone’s friend opened an attachment, installed a certain utility/game, or did nothing at all-and got a wicked virus. The stories undoubtedly end with something along the lines of, “and it formatted the hard disk, destroying everything.” These catastrophic endings are required to get interest high (who would forward, “and it installed an SMTP relay on my computer”?). Of course, the chain letter is completed with a recommendation to tell everyone the recipient knows about this virus; better safe than sorry.

Much of the success of hoaxes is due to the lack of understanding the general public has concerning viruses. That’s understandable, computers themselves are a lot to get a hold on without exploring the code that makes them do things they weren’t intended to do. Computer security as a discipline still enjoys a sense of being a “black art” in many circles; analyzing viruses is magic of the highest order to most users. The lack of awareness programs feeds this problem, blocking viruses and attackers is left with information assurance folks and their toolboxes (including antivirus software) alone. Nonetheless, virus hoaxes are not a tremendous problem for most organizations, outside of a few additional help desk calls regarding the email that someone’s concerned brother sent to warn of the latest viral apocalypse. More damaging to most security efforts is the perception that real viruses can do extraordinary things to a network and devices connected to it.

That is One Magic Bullet

“Virus Voodoo” refers to attributing unrealistic and unproven attributes to a virus, either in the way it spreads or what it does after infection. Constant warnings of virus activity without rational explanations of what to look for or how to protect organization assets perpetuate the lack of understanding. When it comes to managers, CSOs, etc. this

confusion is costly. Often companies react to the mystical threat of a new worm before pinpointing how it spreads, what it can do, and what the infection costs may be. This is not to say that every virus requires a conference call and a midnight meeting, a member of an existing IA team can dismiss most worms before they are escalated to the executive level.

Worms that are not addressed by the current security posture, however, have to be properly examined. There are already reports on infectionvectors.com that detail a process model for dealing with threats and how to analyze the threat of a new virus in terms of real dollars. The point is, don't make decisions that affect the way business is done based on uninformed guesses or wild theories.

Fighting the Voodoo

It is probably clear from the previous articles that the focus should be on sound training and awareness programs; information is the best defense against viral voodoo. See the October 2004 [Focus on Awareness](#) papers and presentation outlines for a good start. In a professional sense, dispelling the voodoo is important so that information assurance maintains a solid reputation as a discipline, not a dark art. That makes it easier to get everyone on the same page of response processes and to avoid the emergency midnight phone calls.

Copyright © 2004 infectionvectors.com. All rights reserved.