



Mass Mailer Threat Modeling & Your Network

infectionvectors.com

September 2004

Overview

Every organization should be aware of what strengths and weaknesses exist within their networks. This type of data is vital to planning for additional virus protection and for mitigation efforts when new threats appear in the wild. Previous documents such as the Malcode Process Model paper describe ways to make use of this data for organizations of all sizes when evaluating threats.

In general, threats that affect the corporate community are quite different from those that concern home users. Mass mailers point out why this distinction exists and make a good study for developing a threat profile for any organization. This report discusses the reasons mass mailers are a greater risk for corporate users than may be expected and how one can build a threat model for their specific network.

Trends in Virus Threats

Mass mailers have been especially popular in 2004, no doubt due to the success and media attention that these worms have had. This success is weighted towards the corporate users. Taking a look at reports from two major AV vendors, Sophos and Panda Software, one can see the distinction between a home threat and a corporate threat. Sophos' "Top Ten" report for August 2004 is comprised of 10 mass mailers. Although there are some additional vectors to each (file shares, PE infection with Lovgate, etc.) each of the worms is classified as a mass mailer and uses email as its primary infection vector.

Panda's "Top Ten" dated September 1, 2004 also points to the differences in the home threat and the corporate threat: Internet worms find plenty of hosts on home/broadband networks, where only the most successful mass mailers are able to crack the list.

This difference is likely a result of a few key factors: perimeter protection, client resources, and security policies for each type of network. Each of these is analyzed in a general sense, i.e.: everyone will know of corporate networks that don't match the assumptions below, this is just meant to be a guide for evaluating the respective networks of the reader.

Perimeter Protection

A home user may consider his/her network perimeter the access device that connects their PC to the rest of the world, whether it's a DSL/cable router, 56K modem, etc. When it comes to securing the machine against Internet worms, this is quite true, the shared segment of cable access may be teeming with malicious code that needs to be filtered (more on this idea below). However, when it comes to email, the ISP's mail servers are more correctly the edge of this service. The ISP likely performs virus scanning and blocking by way of its own security policies. These efforts silently keep many mass mailers away from home users.

In the corporate world, there is generally no default email scanning taking place. Most organizations wouldn't want this service anyway, legitimate email would invariably be dumped which jeopardizes business contacts and profits. Corporations take responsibility for their own filtering (or lack thereof), which often focuses on spam.

Client Resources

Resources, from the worm's perspective, are additional targets to exploit; specifically, this means the number of email addresses that can be harvested. Most home machines do not have the extensive address books of a corporate PC, which probably has access to a company-wide address list. Most of these will be delivered internally as well for a corporate user, meaning the worm will not have to travel to another ISP, where potential virus scanning is taking place (see above).

Security Policies

When it comes to keeping machines patched properly, corporate networks are generally the winners, at least in terms of raw numbers of machines patched. Home machines have been the playgrounds for Internet worms such as Sasser for precisely this reason (as well as the lack of a firewall, etc.). Corporate machines are generally firewall-protected, monitored with an IDS, and managed by software updating tools. Email, however, is of course allowed through all of this and delivered to the gateway/server before being inspected. If there is no gateway scanning in place or the scanning software is not updated frequently, the only protection afforded to the corporate LAN is the client AV software and the security training that each user has been given.

If the network is relying on a single layer of defense (the client AV software) or user training, then the success of the security program is easy to evaluate. It also may make the security engineers a little worried when put in these terms.

For home users the shared medium of cable access may be a very fertile ground for worms like Sasser. ISPs, while adept at scanning for spam and mail-borne worms, will not be able to provide much protection against one's neighbor's infected PC.

Model the Threats

There are a few major classes of malicious code that should be analyzed by every information security officer: mass mailers, macros, and Internet worms. Although it is not cost effective to identify every subset and possible infection vector for each of these, it is possible to identify where they should be stopped in a specific network. Doing so will help determine where additional protection is needed to make the actual security posture match the risk tolerance of the enterprise.

Copyright © 2004 infectionvectors.com. All rights reserved.