Alerts & Vulnerabilities (4):  
Internet Weather Report

by M. E. Kabay, PhD, CISSP  
Security Leader  
INFOSEC Group  
AtomicTangerine, Inc.

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 will look at alerts and vulnerabilities.

The System Administration, Networking and Security (SANS) Institute provides many resources at its main Web site <http://www.sans.org>. Among many other useful services, SANS offers three free e-mail publications of interest to network managers:

- Security Alert Consensus: a weekly digest of new threats and patches;
- Windows Security Digest: the latest system administration requirements for the worlds most widely-used operating environment (distributed monthly); and
- Newsbites: a weekly digest of the editors’ pick of the top 25 security news stories.

To subscribe to these publications, just send an e-mail to info@sans.org with one or more of the following in the subject line: Security Alert Consensus, Windows Security Digest, or Newsbites.

The new SANS Emergency Incident Handler site <http://www.incidents.org/> provides a good summary report on the latest security threats and vulnerabilities. The Incidents.org home page presents a dense summary of breaking news in the security field and currently features a multicolored line graph showing the frequency of probes on specific ports; this graph is one of the products of the concerted effort to map incidents on Internet sites and help to fight widely-distributed attacks. With the collaboration of correspondents throughout the world, SANS’ “Internet Storm Center” can not only track what’s happening but can also supply early warnings to anyone who wants to listen and can supply valuable data to law enforcement officials.

A fascinating case study of the effectiveness of this new tool is reported at <http://www.incidents.org/isw/iswp.php>. On March 22, 2001, participants in the Internet Storm Center project reported a worldwide flood of probes to port 53 (associated with the Domain Name Service). The Lion worm was launching hundreds of thousands of probes automatically; when it found susceptible systems, it infiltrated them and sent password files to a Chinese site, then installed a Distributed Denial-of-Service zombie for later use.

Thanks to the coordination provided by the Internet Storm Center, a global effort to fight the attack began within an hour of the initial reports. The Incident Handler assigned to the problem communicated with cooperating network and security administrators, and within three hours, reports started filtering in of specific infections by the malicious software. Within 14 hours of the initial spike in probes, the Center alerted 200,000 participants to the attack with information on how to identify and stop the worm. Internet access to the Chinese site receiving password files was terminated by UUNET as a result of the worldwide effort.

In addition to the Internet Storm Center, the new Incidents.org site also offers access to well-organized resources from SANS such as the Consensus Intrusion Database, which holds the
voluminous data from intrusion reports used by the Internet Storm Center. The database provides a number of reports of interest, such as the top ten source IP addresses for scans reported to the Center – of great interest in configuring firewalls, for example.

Readers will find a great deal of useful – and fascinating – information from the cutting edge of information security at the SANS and Incidents.org sites. Congratulations to Allan Paller, Stephen Northcutt and all their collaborators on a superb addition to the growing suite of defenses against malicious Internet abusers and their malicious software.

* * *

The next article in this series will focus on some useful resources specializing in identifying new threats from malicious software and distinguishes hoaxes from reality.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For Web-based or CD-ROM online training in security from our Information Security University project, see <http://infosecu.com>.

For information about AtomicTangerine, visit <http://www.atomictangerine.com>.

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.