Computer Security Administration
Computing and Networking Services

Security Incidents Report

October – December 2003

Prepared for: Eugene Siciunas, Director Computing and Networking Services

Background

The Computer Security Administration section of Computing and Networking Services (CNS) prepares this report on a quarterly basis for the information of the Academic Advisory Committee (AcAC) of the Computing Management Board (CMB). Its purpose is to categorize and summarize computer security-related incidents detected and investigated. It is intended that such information will be used to guide the formulation of policies and procedures within the various concerned groups.

For the purpose of this report, security incidents will be grouped in the following categories[1]:

Malicious code: These incidents involve virus, worm trojan program infection and propagation.

Denial of Service: These incidents can be caused by infected computers whose exploit results in a symptom such as the generation of excessive packet rates or continuous rebooting.

Inappropriate Usage is defined by the violation of acceptable use policies and includes cases of email harassment or unlawful use of copyrighted materials

Unauthorized Access to a physical or logical resource without appropriate permission.

In addition to incident reporting, CNS implements Vulnerability Assessment testing which will be discussed in this report.

There are a number of groups within CNS who contribute to security incident handling as well as IT support from academic departments and student residences. These groups participate in data gathering and measurement, incident investigation/forensics and vulnerability assessment.

Overview

This period was marked by the continuous presence of the Microsoft Windows Welchia virus. Numerous academic and student residence subnets were infected to the point that ICMP filtering was required at the router borders to the core

[1] Computer Security Incident Handling Guide, National Inst. Of Standards and Technology, Pub. 800-61

network. Infected host lists were compiled hourly and made available on the CNS Network Operations website. Numerous announcements were made on the two network admin mailing lists to keep staff up to date on host infections.

Vulnerability Assessment

CNS runs vulnerability scans campus-wide bi-monthly for the most current and serious issues as given by the SANS Top20 List. The results are used to generate a list sorted by department administrator who then uses the list to remove the vulnerabilities.

Scan Results for RPC DCOM Vulnerability Fixed by Patches MS03-039

Date of Scan	Hosts Vulnerable
Sept. 15-16	6079
Sept. 17	4111
Oct. 1-2	2458
Oct. 14	1728
Nov. 6	1873
Nov. 24-25	1554
Dec. 12	1210

Scan Results for Windows Messenger Vulnerability Fixed by Patches MS03-043

Date of Scan	Hosts Vulnerable
Oct. 17-18	2778
Oct. 23	3253
Nov. 3	2823
Nov. 26-27	1770
Dec. 12	1210

Scan Results for rsync Remote Vulnerability

Date of Scan	Hosts Vulnerable
Dec. 10-11	28

Scan Results for Weak Password Vulnerability

Month	Detected Instances
July	112
August	32
September	N/A
October	75
November	N/A
December	181

Up to this point, there has been no attempt to follow up on vulnerability assessment reporting. It is not known which departments are using the reports as an aid in the cleanup of vulnerable systems. Obviously, after the onslaught of the Blaster and Welchia worms which exploited the RPC DCOM vulnerability, the number of vulnerable hosts decreased rapidly but seemed to plateau at 1000. An attempt will be made to reduce this number of vulnerable machines while, at the same time, determine if some improvements to notification should be made.

Virus/Worm Incidents

Virus outbreaks are detected by CNS or University IT staff by monitoring world-wide security incident mailing lists such as those from securityfocus.com or by detecting abnormal traffic patterns in network traffic or system log files. Such incidents are announced on the network admin mailing lists. Worm propagation is often detected similarly – network traffic signatures are made available on security incident mailing lists and are used in intrusion detection systems to identify infected hosts.

Virus/Trojan	Detected Instances	Characteristics
Autoproxy	4	http/socks proxy and sends SPAM
Pseudo Coreflood	12	Unpatched IE, http proxy, sends SPAM
Qhost	18	DNS requests
Welchia	250	ICMP traffic
Blaster	40	Propagation traffic

Inappropriate Usage

The highest ranked classification of Inappropriate Usage by detected instances is Copyright Violations. Agencies, hired by American movie studios, are detecting IP addresses that act as file-sharing servers for movies. They contact the University and generally ask that the detected user stop using the copyrighted material in question. These instances appear to be on the increase. The policy for dealing with these incidents is to notify the network administrator of the issue, ask them to verify that the occurrence took place. If so, then the user involved is asked to stop using the material. Also, the department chairman/dean is notified of the incident.

Classification	Detected Instances	Characteristics
Copyright Violations	14	Movie sharing
Malicious or Fraudulent Email	5	
SPAM Source	1	