Computer Security Administration
Computing and Networking Services

Security Incidents Report

January – March 2004

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.

Period Summary

The start of this period was marked by the disappearance of the Welchia worm due to the programmed termination date of Jan. 1 2004. The worm, which exploits the Microsoft Windows DCOM vulnerability, began causing network

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

problems, specifically ICMP degradation of service, in September, 2003. While infected network administrators worked on repairing hosts, ICMP limiting filters kept outbound traffic to a minimum at the cost of non-existent ICMP performance for valid applications. This performance has now returned to normal. Another major network-related incident began in March and involved intermittent loss of operation of 3Com switches. Two bugs were found in the switch firmware, one of which involved a buffer overflow condition in the internal web server which caused the device to reset regularly on receipt of exploit traffic. This traffic was not directed specifically to the switches. The numerous resets resulted in denial of service conditions for many campus users. By the end of March, the vendor supplied a patch to remedy the problem.

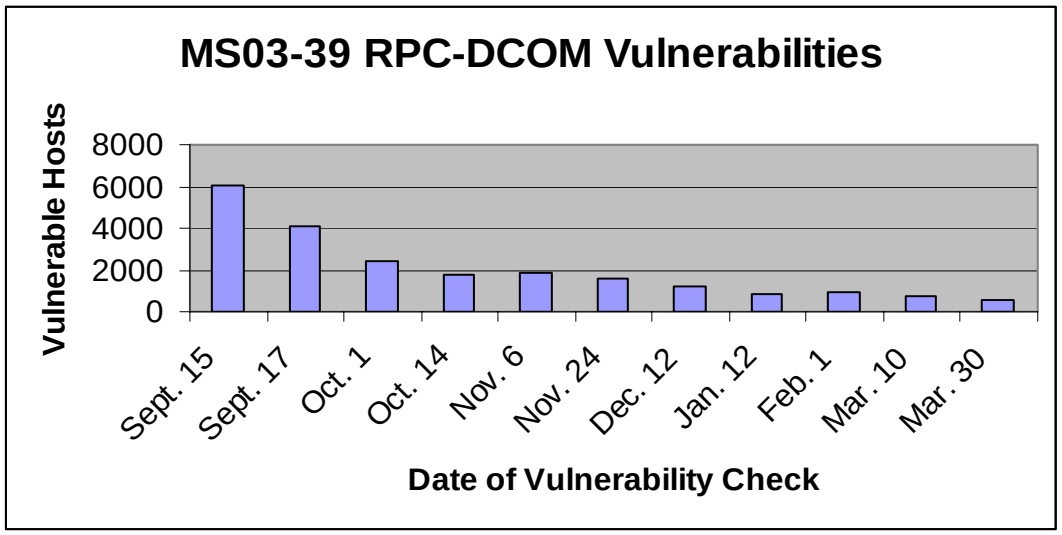
Spam and virus prevention activities held a high priority over the period. CNS staff successfully brought into production the Sophos PureMessage anti-spam product on its UTORmail systems. This service redirects unsolicited commercial email which originates external to the University, a big source of which is due to external compromised hosts. Network Services staff evaluated an anti-virus component to the Sophos product for three weeks. The January evaluation period was timely – the product was a key factor in reducing the effect of major outbreaks of MyDoom, Bagle, and Mimail. February saw two new viruses introduced – Sober and Netsky.

This period saw a large increase in the number of reports of copyright violations – mainly from movie studio agents. It is not known whether the increase is due to poor policy compliance by University users (mainly from student residences) or more effective monitoring by the agents.

Vulnerability Assessment

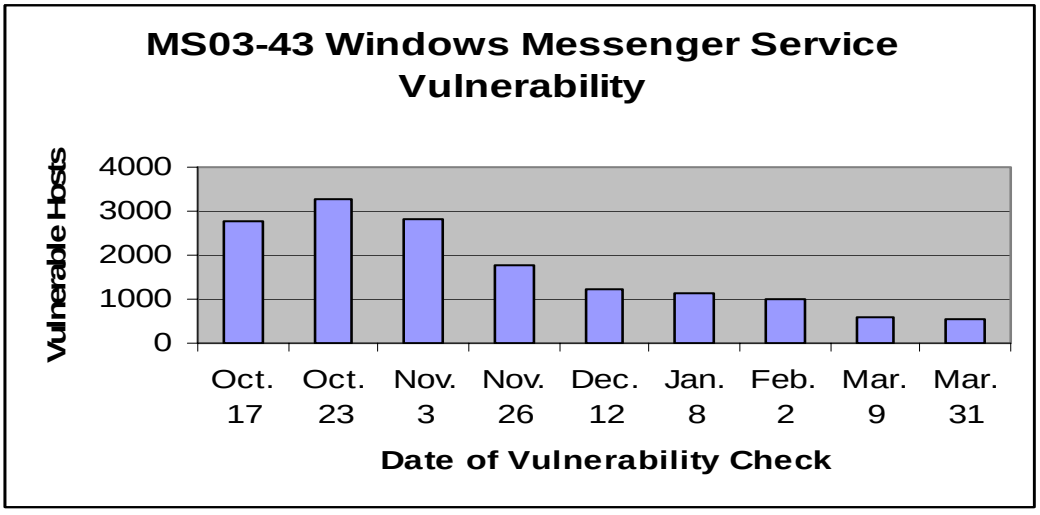
CNS runs vulnerability scans campus-wide bi-monthly for the most current and serious issues as given by the SANS Top20 List.

Scan Results for RPC DCOM Vulnerability



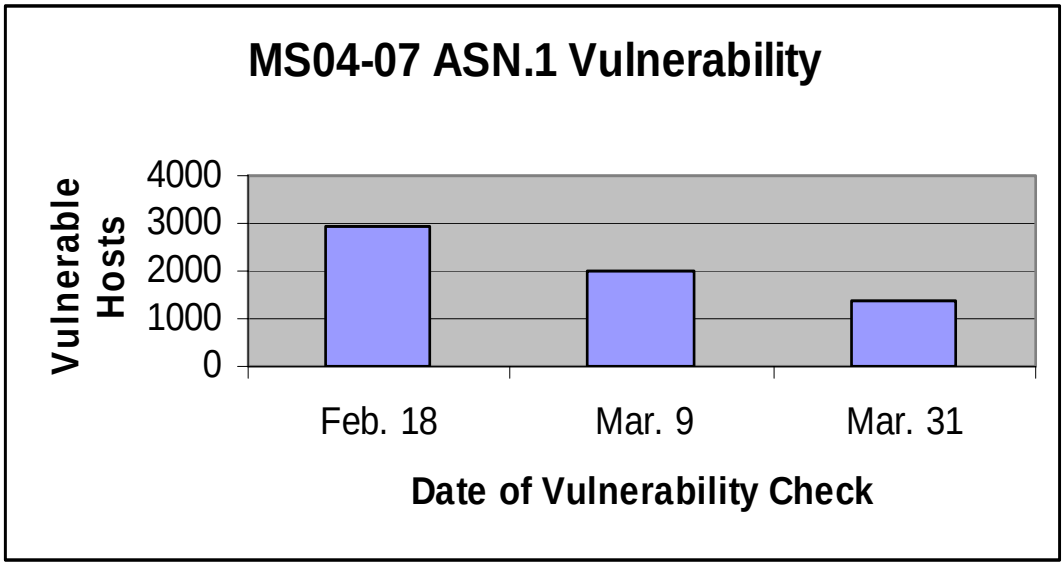
The MS03-39 vulnerability was exploited by the Blaster and Welchia worms and continues to be targeted by current 'bot' attacks so efforts continue to encourage department administrators to patch vulnerable hosts. This is done in two ways: reports of scan results for a department are made available on a website and the administrator is notified, and departments with the largest number of vulnerable hosts are contacted directly to be reminded not to neglect patching.

Scan Results for Windows Messenger Vulnerability



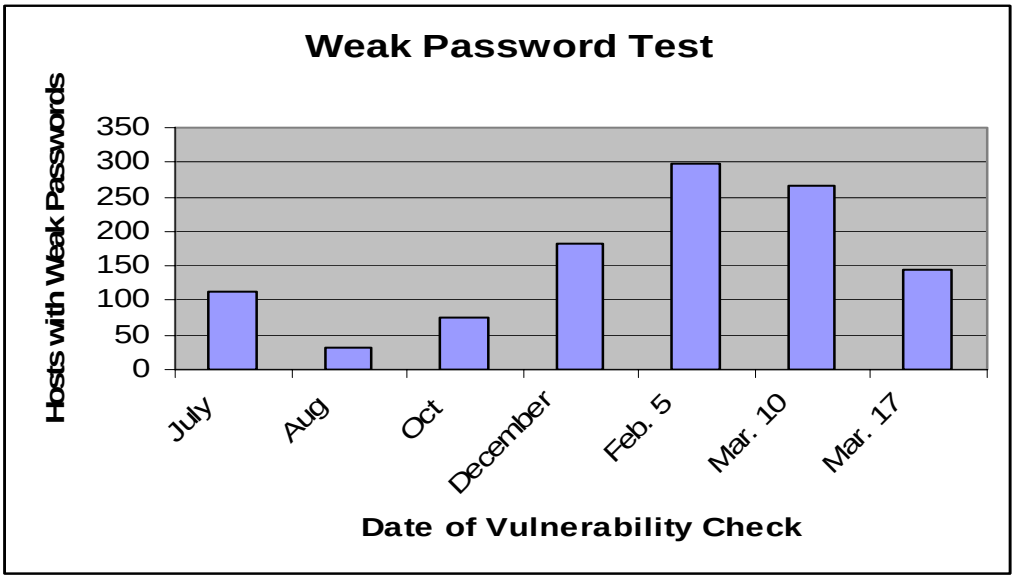
There are a number of tools available to exploit this vulnerability.

Scan Results for Windows ASN.1 Vulnerability



There are no known tools that exploit this vulnerability.

Scan Results for Weak Password Vulnerability



Password checks fail when there is no password associated with a user or the password is the same as the username.

Virus/Worm/Trojan 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.

This period has seen the detection of 'blended threat' trojan bots. These exploit tools contain multiple commands which attempt gain access using all available vulnerabilities. Once installed, they are known to damage the host, generate DoS attacks, and do packet sniffing. The Agobot is especially dangerous because of its ability to do brute password attacks. Other bot variations are reported to do keystroke capturing.

Virus/Trojan	Detected Instances	Characteristics
Pseudo Coreflood	28	Unpatched IE, http proxy, sends SPAM
Welchia	0	ICMP traffic
Blaster	0	Propagation traffic
Phatbot	25	Blended threat: exploits MS03-39, 03-43, MyDoom backdoor, Beagle backdoor
Agobot	10	Blended threat: same as Phatbot with password guesser

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		Movie sharing
Oct – Dec 2003	14	
Jan – Mar 2004	67	
Malicious or Fraudulent Email	0	
SPAM Source	2	