---------FOR INFORMATION ONLY---------

WORM VIRUS INFECTION

On January 25, 2003 a server on the Plant Network was thought to be infected with the MS-SQL Server Worm. The consequence of the infection was large amounts of data sent onto the site network. The large amounts of data caused many computers to cease from communicating with other computers on the network. Both the Business network and the Plant network were affected by the consequence of the MS-SQL worm.

The slow network response was initially noticed in the morning, around 09:00 on the Business network. It wasn't until after 16:00 that degradation in response time of computers was noticed on the Plant Network. The Safety Parameter Display System (SPDS) became unavailable at 16:50. The Plant Process Computer (PPC) became unavailable at approximately 17:13. The unavailability of SPDS and PPC was burdensome on the operators. Also the loss of SPDS for more than eight hours requires the NRC be contacted.

MS-SQL WORM

The MS-SQL Worm released onto the Internet by some unknown source on January 25, 2003 targeted the MS-SQL Server vulnerability through port 1434/udp.

The worm targeting SQL Server computers is self-propagating malicious code that exploits the following documented vulnerability in Microsoft SQL Server 2000.

Microsoft SQL Server 2000 contains a remotely exploitable stack buffer overflow that allows attackers to execute arbitrary code with the same privileges as the SQL server.

The SQL Server Resolution Service (SSRS) was introduced in Microsoft SQL Server 2000 to provide referral services for multiple server instances running on the same machine. The service listens for requests on UDP port 1434 and returns the IP address and port number of the SQL server instance that provides access to the requested database.

The SSRS contains a stack buffer overflow that allows an attacker to execute arbitrary code by sending a crafted request to port 1434/udp. The code within such a request will be executed by the server host with the privileges of the SQL Server service account.

This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account. If the privileges of the service account are elevated through a SQL Server vulnerability, this vulnerability may result in compromise of the server host.

This vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow.

Once the worm compromises a machine, it will try to propagate itself. The worm will craft packets of 376-bytes and send them to randomly chosen IP addresses on port 1434/udp. If the packet is sent to a vulnerable machine, this victim machine will become infected and will also begin to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no other payload.

Activity of this worm is readily identifiable on a network by the presence of 376-byte UDP packets. These packets will appear to be originating from seemingly random IP addresses and destined for port 1434/udp.

NETWORK PROTECTION

Computer Engineering was informed by Network Services that the Corporate firewall filters incoming and outgoing packets to port 1434/upd. This filter does not allow packets going to or coming from port 1434/upd to pass through the firewall. Therefore the Worm did not come through the Corporate Internet connection to the Plant internal network.

MS-SQL SECURITY PATCH

It was discovered that an external consultant has a T1 data communication link to the Corporate's internal network. Also the consultant has it's own separate DSL connection to the Internet. This is in essence a backdoor from the Internet to the Corporate internal network that was not monitored by Corporate personnel. During this discovery Computer Engineering and Client Services became aware that some people in Corporate's Network Services department were aware of this T1 connection and some were not.

According to the Internetworking Security Policy, Information System Letter No. 7, dated May 1996, it requires a security system to be in place for external sources to access Corporate's internal network. The policy further defines what the security system will be based on access requirements. Based on the information received during the investigation, this Policy was not enforced with respect to the T1 connection.

Computer Engineering has concluded that it is very likely that the server was infected with the MS-SQL Worm.

The external consultant who has a link to Corporate's Intranet, provided the application software currently being run on the server. The consultant also reported that this Worm impacted their servers within their company.

It was discovered the security patch that removed the vulnerability target by the MS-SQL Server Worm was not installed on the server. Therefore the server was vulnerable to the attack. The security patch for this vulnerability was documented and released by Microsoft on July 10, 2002.

The SPDS was unavailable for approximately 4 hours and 50 minutes. The Plant Process Computer was unavailable for 6 hours and 9 minutes. The event was not significant because the control and protection functions were not affected.

APPARENT CAUSES

The Apparent Cause is the combination of four causal factors. The removal of any one of the first three would have prevented the event. These casual factors are:

1. MS-SQL Worm Released on the Internet

Microsoft details fully the vulnerability of their product when they release a patch to fix the problem. Therefore hackers throughout the world are given full information of how to target these vulnerabilities. The security patch for the vulnerability targeted with the MS-SQL Worm was released in July 2002. This gave the hacker(s) 6 months to develop a Worm to target the vulnerability documented by Microsoft.

Remedial Action:
No Actions will prevent the release of viruses or worms from individuals throughout the world.

2. Less Than Adequate Control of External Connection(s) to Corporate's Internal Network

The corporate connection to the Internet passes through a firewall. This firewall is used to keep unwanted communications from entering Corporate's Internal Network. A Network Services person stated the firewall filters packets 1434/udp. Therefore the MS-SQL Worm did not enter through the formal corporate Internet connection but through another opening. Further investigations showed there are additional external connections into Corporate's Internal Network that are not monitored at the same level as

the firewall. Also speaking to a number of personnel within the Network Services department it became apparent there is not a thorough knowledge of all external connections that exist to Corporate's internal network.

Remedial Actions:
1. Network Services shall document all external connections to the Internal Network, and monitor and filter the connections to the same standard as the corporate firewall.
2. Install a firewall between the Plant network and the Corporate network.

3. Security Patch not installed on Server in a Timely Manner
On July 10, 2002, Microsoft released a security patch and information on the vulnerability that the MS-SQL Worm targeted on January 25, 2003. Had the security patch been installed on the server, it would not have been a target of the MS-SQL Worm.

Remedial Action:
1. Immediate action taken was to shutdown the server. Since the MS-SQL Worm was only memory resident, shutting down the server removed the Worm from the server's memory. The server then was no longer infected.
For precautionary reasons, the server was isolated from the site network. The server was then powered on and the security patch was installed. The server was then reconnected to the site network.
2. It is imperative that when security patches are released for software products used at the Plant, they be installed as soon as possible.

4. Computer Engineering personnel not aware of Security Patch
There is currently no formal process in place for personnel within Computer Engineering to be made aware of security patches issued for the systems supported. Individually Computer Engineering personnel may browse Microsoft's and other vendors web site for released security patches.

Remedial Action:
A process shall be setup for personnel within Computer Engineering to review security patches for the systems they support.

RECOMMENDED CORRECTIVE ACTIONS

1. Network Services shall document all external connections to the Internal Network, and monitor and filter the connections to the same standard as the Corporate firewall.

2. Firewall shall be installed between the Plant network and the Corporate network.

3. Implement a process that will provide Computer Engineering personnel the opportunity to review security patches for the systems supported and install them in an acceptable time frame.

Mail Envelope Properties (3E8B6B15.8AD : 22 : 30893)

Subject: Worm Virus Infection Paper
Creation Date: 4/2/03 6:02PM
From: <drwuokko@firstenergycorp.com>

Created By: drwuokko@firstenergycorp.com

Recipients
nrc.gov
owf4_po.OWFN_DO
JBH1 (Jon Hopkins)

firstenergycorp.com
pjmccloskey CC
mkleisure CC

Post Office	Route
owf4_po.OWFN_DO	nrc.gov
	firstenergycorp.com

Files	Size	Date & Time
MESSAGE	90	04/02/03 06:02PM
Worm Virus Infection.rtf	22993	
Mime.822	32875	

Options

Expiration Date:	None
Priority:	Standard
Reply Requested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard