Global Information Assurance Certification Paper

Enterprise-Wide Virus Protection

(So You Think You're Protected from Malicious Code!)

Bob Mallion

November 20, 2000

Case Study:

On a bright sunny day when all was going well, the alert alarms from all of the four Exchange E-mail Servers interrupted the daily routine of intrusion detection log monitoring, policy updating, addressing "ad hoc requests" to punch holes in the firewall for reasons of user convenience, and other activities that typically occupy the time of Automated Information Systems (AIS) security personnel.

As the manager of the AIS Security Program Support Office, I quickly reviewed and identified the event as a *real* incident (as opposed to a false positive identification of malicious code in an e-mail attachment). In addition to activating our Incident Response Team, which within two minutes, shut down all e-mail transfer services to isolate the outbreak, I began an investigation of the incident. The goal: 1) to determine the cause of this denial of service (DoS) attack; and, 2) to determine how or if it could it have been prevented?

The event occurred in September at a research and development (R&D) facility implementing the following mix of hardware and software:

- 4 "security hardened" Compaq Proliant NT Exchange E-mail Servers
- Microsoft Exchange, Version 5.5
- Norton Anti-Virus for Exchange 2.0 (NAVMSE)
- Multiple Anti-Virus Software Applications for desktops deployed throughout the enterprise environment (e.g., Norton, McAfee, F-Prot, E-Safe, etc.).

While we know there are no guarantees when it comes to Information Systems Security (ISS), significant efforts were made at the facility to implement a cost-effective Anti-Virus Program (AVP). Members of the AIS Security Program Support Office and desktop support personnel (9 staff in total) routinely check the antivirus software vendors sites daily, and provide updated signature files and application upgrades for the network and e-mail servers, and the approximately 1,250 person end-user community.

So why was there a DoS incident at the site? Malicious code is becoming more sophisticated and takes advantage of previously unknown and unused vulnerabilities. In this case, it has been determined that one of the culprits was *speed*. The combination of hardware and software was simply unable to handle the speed at which the distribution of the infected mail was occurring.

Incident Details:

A facility employee who: 1) *had attended* a general awareness security seminar; 2) *was aware* of the importance of opening files from unknown sources; and, 3) *had **not** installed* the most recent signature files made available to end users, was reviewing files on a shared project disk. The project was related to the stages of a systems life cycle, and upon finding a mail message entitled "Life Stages"…. Well, you can imagine the rest.

Thousands of messages later (most of which had been intercepted by the scanning tool), the clean up began. However, it was determined that as many as eight infected messages had "leaked through" the scanner and had been delivered locally. That's right, eight local recipients – there was no way of knowing how many messages may have made it to other destinations.

While the staff was cleaning up the impacted systems, recipients of the "leaked through messages" were opening their e-mail and re-infecting the systems (though these distributions were isolated to his/her primary server environment). Approximately six hours later, a full sanitization of the systems was completed and all facility e-mail services were restored.

Research:

At the time the event was taking place, very little could be found to assist in the investigation. Subsequent research has provided enough information to determine the cause. The following supports my conclusion:

- Microsoft Exchange Server, version 5.5 utilizes the Messaging Application Programming Interface (MAPI). This allows the scanning of mail as it arrives in the mailbox's inbox. With the release of a plug-in for Service Pack 3 of this version, Microsoft introduced the Virus Application Programming Interface (VAPI). This allows for the monitoring of e-mail attachments within the Exchange Information Store, thus "seeing" all mail before any other process or application.[1] (The site in this study had implemented the MAPI mode, as at the time of the incident, the VAPI plug-in was not available.)

- The vulnerability exists in that when an Exchange Server is experiencing a heavy load, a third party anti-virus application may not be notified of incoming messages by MAPI. It is thus possible that the scanning software will not detect an infected attachment to a mail message and a user can receive an infected attachment before the attachment is scanned and repaired by the anti-virus package. Should an infected attachment be modified while attempting to repair it, the anti-virus package simply creates a log entry indicating that an infected attachment was detected and no further action is taken. The infected file may still be able to deliver its payload.[2] In this case, it did!

---

[1] Knowledge Base; Norton AntiVirus 2.x for Microsoft Exchange; *Summary of the three different Auto-Protect modes available in Norton AntiVirus for Microsoft Exchange 2.1*; Document ID: 2000091515511106;

[2] Knowledge Base; Symantec; *Sometimes Worm Viruses Are Not Detected With The Real-Time Scanner In Norton AntiVirus For Microsoft Exchange*; Document ID: 1999052509370406; Date Created: 05/25/99; Last Modified: 09/18/2000.

Addressing the Vulnerability:

Recently (September-November, 2000 timeframe), Microsoft acknowledged there is an issue related to the Exchange Server 5.5, SP3 software. The R&D facility has installed the Microsoft upgrade that allows for the use of the VAPI solution to the fast replication issue.

All is well! Hardly!

With the introduction of VAPI by Microsoft, and the upgrade to new releases of anti-virus software by vendors to implement VAPI, additional issues have arisen. The facility has recently been experiencing some difficulty with mail services in sending and receiving some e-mail messages.

- E-mail messages are not being sent.

  When you send an e-mail message, the message may not be sent and may remain in the Outbox. This behavior only occurs when you use a third-party antivirus scanning program that uses the antivirus application programming interface (VAPI) that was introduced in Exchange Server Service Pack 3.[3]

  No solution is available at this time.

Also, employees at the facility have been sent malicious code which can not be traced (but can be deleted by AV software).

- Malicious code cannot be traced.

  From the perspective of an AIS Security Manager, it is important to be able to trace the source, the recipients, and the type of malicious code when an incident occurs. What then can you do with the following information?

  Sender of the infected attachment: Unknown Sender
  Recipient of the infected attachment: Unknown
  Subject of the message: Unknown

  Answer: Not very much.

It's true! In some environments, this is the only information available in the logs. Thus, it's impossible to investigate/audit the incident.

[3] Microsoft Product Support Services; Article ID: Q263947; XADM: Messages Stuck in Outbox with Antivirus Application Programming Interface in Use; Last Reviewed: November 8, 2000

Conclusions:

Even though steps are taken to protect the enterprise, malicious code can still pose a serious threat. As in the proverbial "chain" simile, efforts at antivirus remediation can only be as effective as the weakest link. It is felt that this event *could not have been prevented*, as the software vendors did not acknowledge there was a problem until after we had experienced the denial of service attack.

Lessons Learned/Confirmed:

What can be learned/confirmed from an event of this type?

1. Every environment is vulnerable to malicious code from multiple entry points: workstations, network servers, Internet e-mail gateways, and firewalls.

2. Maintaining enterprise-wide virus protection is an on-going, resource intensive undertaking.

3. With the proliferation of malicious code today, it is nearly impossible to:

   - Ensure all workstations are running current anti-virus software;
   - Ensure all network servers, Internet e-mail gateways, and firewalls are running current anti-virus software;
   - Ensure anti-virus software is properly configured to provide full protection;
   - Ensure complete protection against malicious code when it invades an enterprise.

4. Even though personnel have received appropriate awareness and training in the use of systems, they can be a vulnerability to your environment.

5. Central management of a Virus Remediation Program is not reliable unless all systems are properly configured and maintained. Configuration management is necessary, as is system standardization.

6. Distributed management of a Virus Remediation Program is not a reliable solution. Too many variants in the program can cause integration problems.

7. Exchange Mail Server antivirus application software cannot be relied upon as a first

line of protection for your enterprise environment.

Bibliography:

Knowledge Base; Norton AntiVirus 2.x for Microsoft Exchange; *How to use background scanning with Norton AntiVirus for Microsoft Exchange 2.1;* Document ID: 2000091516493606; Date Created: 09/15/2000; Last Modified: 10/11/2000.
http://service1.symantec.com/SUPPORT/nav.nsf/361fc4a260e563b1882568180069e1c0/8f1034e244189ce68825695b00829650?OpenDocument&Highlight=0,nav,2.1

Knowledge Base; Norton AntiVirus 2.x for Microsoft Exchange*; Norton AntiVirus for Microsoft Exchange 2.1 Reports Known Sender And Receiver When Set Up To Use VAPI Or VAPI/MAPI*; Document ID: 2000092807270206; Date Created: 09/28/2000; Last Modified: 10/04/2000.
http://service1.symantec.com/SUPPORT/nav.nsf/361fc4a260e563b1882568180069e1c0/644c9983cd78955b88256968004f325e?OpenDocument&Highlight=0,unknown

Knowledge Base; Symantec; *Sometimes Worm Viruses Are Not Detected With The Real-Time Scanner In Norton Antivirus For Microsoft Exchange*; Document ID: 1999052509370406; Date Created: 05/25/99; Last Modified: 09/18/2000.
http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999052509370406

Knowledge Base; Norton AntiVirus 2.x for Microsoft Exchange; *Summary of the three different Auto-Protect modes available in Norton AntiVirus for Microsoft Exchange 2.1*; Document ID: 2000091515511106; Date Created: 09/15/2000; Last Modified: 10/10/2000.
http://service1.symantec.com/SUPPORT/nav.nsf/361fc4a260e563b1882568180069e1c0/268a6872e6560c138825695b007d3d3c?OpenDocument&Highlight=0,nav,2.1

Microsoft Product Support Services; Article ID: Q263949; XADM: Understanding How the Antivirus API Scans Attachments; Last Reviewed: October 18, 2000;
http://support.microsoft.com/support/kb/articles/Q263/9/49.ASP

Microsoft Product Support Services; Article ID: Q263947; XADM: Messages Stuck in Outbox with Antivirus Application Programming Interface in Use; Last Reviewed: November 8, 2000
http://support.microsoft.com/support/kb/articles/Q263/9/47.ASP

Discussions with Systems Security Personnel and Administrators of E-mail Servers at:
SANS NS2000, Monterey CA, October 15-22, 2000;
Both government and corporate facilities.