Global Information Assurance Certification Paper

"AnnaKournikova Virus" - Lessons Not Learned by John Appleby

By the time most of us saw the evening news on Feb 12th 2001 we were all very aware of the "AnnaKournikova" virus. While the "AnnaKournikova" virus was not a newly discovered virus, nor was it vastly different from the "Loveletter" virus in its mode of deployment, many corporations had their e-mail operations severely impacted by the "AnnaKournikova" virus. The purpose of this paper is to analyze why this virus was so successful in the light of the lessons that should have been learned from the "Loveletter" virus episode.

AnnaKournikova Virus Characteristics

This virus is a Visual Basic Script (VBS) that was created by a worm-generating tool. In this instance I have used the terms virus and worm interchangeably, as do the Anti-Virus vendors [1], however see Wing [2] for a discussion of whether VBS malware [3] should be classed as a virus or worm.
When run the script copies itself to the WINDOWS directory, attempts to mail a separate e-mail message, using MAPI messaging, to all recipients in the user's Microsoft Outlook Address book. Consequently this virus has the potential to create e-mail storms that can slow down general network performance and severely impact the performance of e-mail servers. These characteristics are so sufficiently similar to the characteristics of the "Loveletter" virus that I will start with a discussion of what measures should have been put in place following that episode.

"Loveletter" Virus Incident

The "Loveletter" virus made its appearance on May 4th. 2000, and its' release was significant because it spread rapidly, and impacted e-mail servers worldwide. This was not the first virus to generate e-mail from the Outlook Address book [4], but its' mode of attack was new and it generated e-mail to every user in the Outlook Address book. The resulting e-mail floods shut down exchange servers for days while servers were cleaned and patched. As a result of this attack many of the technical vulnerabilities that fueled this incident have been addressed.

Technical Vulnerabilities

For the purpose of this discussion technical vulnerabilities are defined as previously undetected, or unreported, software vulnerabilities exploited by malware.

Microsoft Outlook

Following the "Melissa" and "Loveletter" virus incidents Microsoft released a "Security Update" to "provide a higher degree of security" [5] in Outlook 98 and Outlook 2000. The security update blocks users from opening attachments that contain certain file types that are commonly used to distribute malicious code.

Also the security update can block external programs from accessing the Outlook address book without user intervention. Additionally the security update heightens the Outlook default security settings helping to prevent users from spreading VBS viruses.
While this Security update does provide a higher degree of security it can limit the functionality of Outlook. As this product cannot be easily uninstalled Microsoft recommends an examination of the benefits of this product prior to installation.

Anti-Virus Software

Anti-Virus software is somewhat analogous to the influenza vaccine. The Anti-Virus software companies research new trends and try to predict what the form the newest virus attacks will take, additionally their products provide protection against all known viruses and their variants. As with influenza vaccine, anti-virus software cannot protect you against totally new viruses - a technical vulnerability. In response to the "Loveletter" virus incident the anti-virus software companies added VBS files to the list of default files that they screened by issuing updated scanning engines. On the older versions of the scanning engine the VBS files had to be added to the list of scanned files.
Additionally many corporations took the opportunity to examine and implement a layered approach to Virus scanning. It is no longer sufficient to just have virus scanning on the workstations and the servers, a layered approach (defense in depth) is needed. Specific products have been designed to scan mail at the Exchange server, and scan files at the Firewall. By scanning at the firewall and at the Exchange server all but the newest virus attacks can be stopped before they reach the end-user desktop. For an added layer of "comfort" many corporations purchase product from different Anti-Virus vendors for each of these layers of defense.
i.e. Firewall Anti-Virus product from company X
Exchange Anti-virus product from company Y
Server and Workstation Anti-virus product from company Z

While technical vulnerabilities do exist in all software products most software companies respond in a timely fashion with updates, patches, and fixes for these vulnerabilities. Unfortunately organizational vulnerabilities within corporations can lead to these technical vulnerabilities existing long after they have been remedied.

Organizational Vulnerabilities

Organizational vulnerabilities for the purpose of this discussion are defined as inadequate or incomplete responses to well documented technical vulnerabilities

Anti-Virus Software

While newly discovered viruses expose the technical vulnerabilities of anti-virus software it is the organizational vulnerabilities of companies to virus incidents that are of a bigger concern. If anti-virus software is installed and correctly maintained most corporations will be adequately protected against all but the newest virus exploits. Correct maintenance of anti-virus software includes not only updating virus definition files on a regular basis, but also upgrading the virus-scanning engine periodically. However, the scale of the recent "AnnaKournikova" incident would suggest that many corporations are failing at these necessary tasks.

Updating anti-virus software and virus definition files in a small company can be a time consuming task, in a corporation with hundreds or even thousands of desktops it can quickly become a seemingly insurmountable task. For this reason many desktop computers are infrequently, if ever updated. Many anti-virus software companies have responded to this situation by providing configuration options that, if enabled, periodically update the virus definition files and the virus-scanning engine. While this works well if enabled, I have found that users will quite often disable this functionality - even to the extent of disabling the software. As a result I have found that pushing the updates out to the users is a more effective solution, most Anti-Virus Software companies offer a software management program [6] to effect the distribution of software and definition files. The advantage of these types of programs is that they enable central control of the process, and provide reports of current status and version (scanning engine and definition files) of the software loaded on each computer. Firewalls, mail servers, and server farms demand extra vigilance - a strict policy should be in place to ensure that the virus definition files are updated weekly (at a minimum), the process can be automated but should be manually verified.

Anti-Virus Response Teams

The "Loveletter" virus incident should have demonstrated to most corporations the need for implementing an anti-virus response procedure. This procedure should be well documented, readily available, and understood by all response team members. The procedure should define how to identify a virus emergency, define what steps to take, and most importantly empower all team members to act in the absence of the "normal" chain of command. The procedures must contain elements of the following - isolate, inform, identify, discuss, remedy, notify, and review. The order I have chosen caused much discussion among team members in my corporation, specifically my placing "identify" third in my list. In the first few hours of a major virus incident it is very difficult to access the web sites of the Anti-Virus software vendors, often making it difficult to obtain an identification and fix for a new virus. Consequently in a major virus incident the first step should be to isolate and contain the damage.

Isolation often means disconnecting the workstation, server, or network segment to stop further dissemination of the virus. These procedures should contain explicit instructions - for instance a team member may not know how to shutdown

a firewall but they can remove the CAT5 cable from the Internet Router if everything is clearly labeled. An Exchange server can be isolated from the network in similar fashion if necessary.
Once the problem has been isolated all employees of the corporation must be informed that there is a problem, what systems or services are unavailable, and if available include explicit instructions on how to avoid compounding the incident. Multiple modes of communication should be used - post notices on all entrances to the office, leave voice-mail messages, use e-mail if available, call designated staff members in each department.
Once the incident has been isolated and information disseminated, then the identification process can begin. Generally by the time the Anti-Virus Software vendors can be contacted the details of the virus and the mode of attack are known. At this stage updated definition files may, or may not be available. Once the identity of the virus is established then it is time to take a break and discuss everything that has occurred up to this point in time. The next step is to remedy the situation by downloading and then applying the patches and definition files necessary to prevent the virus from doing further damage.
Once the situation has been remedied then it is time to notify the user community that services have been restored. Finally, follow-up with another meeting to discuss the complete event including what actions were taken, work through the procedures to see if they need modifying. These meetings must take the form of a learning experience – not blame assignation!

The procedure listed above is based on input from team meetings following the "loveletter" incident at my corporation and contains the elements of a procedure for addressing major virus incidents. However, each corporation should develop procedures that are meaningful to their corporate environment.

E-mail Policies

E-mail has become the lifeblood of a corporation. However, because of the need to extend the reach of E-mail outside the protective (hopefully!) confines of the corporate network, E-mail has become the main mode of transmission of viruses. Now if anti-viral defenses are in place and well maintained, then E-mail poses a reduced threat as a transmitter of viruses. However new viruses can easily penetrate these anti-viral defenses, and unless all E-mail recipients understand what role they can play in stopping the spread of viruses these new viruses can have catastrophic effects on the corporate computing environment. An E-mail policy should be part of the corporate computing policy. A good policy should explain how E-mail is to be used, and explain the dangers of opening unsolicited e-mail. Unfortunately most users rarely review this policy after their first day at work. Consequently it becomes important to remind everyone, on a regular that unsolicited e-mails must be deleted. Appendix A has an example of the reminder that is sent to everyone at my corporation on a monthly basis - the message is fairly generic, and most importantly gives the user the permission to delete unsolicited e-mail regardless of the origin.

Lessons Learned?

. A major incident such as the "Loveletter" virus should have resulted in all corporations reviewing their responses to the incident. Organizational vulnerabilities exist because of inadequate review processes following exploitation of a technical vulnerability. Additionally even if the review processes occur, many corporations fail to act on their findings and remedy known vulnerabilities. Corporations must pay more that lip service to adequate anti-virus defenses. It is imperative that corporations address organizational vulnerabilities that enable such attacks to be successful. The people on the front lines of responding to these attacks need to be provided with necessary resources to fend off these "copy-cat" type attacks. The cost of responding to virus incidents in manpower and lost production far outweighs the cost of anti-virus software and the associated maintenance and distribution programs. If there is management resistance to implementing these types of programs then find out the dollar cost in lost production - business managers understand these types of numbers! For instance if a department keeps asking when E-mail will be back up, then find out why it is so important to them - perhaps this is the last day for a proposal to be submitted that might generate several million dollars for the company. This kind of information can help you make the case for a good, layered anti-virus defense.

Once these anti-virus defense programs are properly funded then they must be implemented and maintained. The best defenses are useless if they are outdated - if we are going to demand the best tools to adequately defend the corporate computing environment from virus incidents, then we must focus our efforts on maintaining these defenses and keeping updated on all new exploits and vulnerabilities. Subscribe to security newsletters [7], anti-virus newsletters [8], visit web sites that have virus information [9] and visit the web sites of all the major software vendors at least weekly. This information is invaluable; just because your anti-virus software can detect a virus doe not mean you are safe - take a few minutes to see what vulnerabilities are being exploited and fix those vulnerabilities!

Conclusion

New virus exploits provide a major challenge to the integrity of corporate computing systems. In the absence of an anti-virus remedy, the corporate users are the first line of defense and educating users to be suspicious of unsolicited e-mail should be an on going process. Once a remedy is discovered and applied to the entire corporate computing environment then theoretically these systems should be secure - until the next new exploit. Unfortunately organizational vulnerabilities cause many corporations to fall victim to repeated virus attacks on their corporate systems.

The worm-generating tool [10] used to create the "AnnaKournikova" incident demonstrates that anyone can unleash a virus. Such a tool however, by its nature, exploits known technical vulnerabilities. This virus family was first

detected in August 2000, and some anti-virus software companies have had updated definition files available for the past six months [11]. Therefore we will continue to see such virus incidents as long as corporate management, and the employees tasked with protecting the corporate data, allows organizational vulnerabilities to exist. If your corporation was affected by just such an incident then it is time to review your procedures and fix them - now!

References

[1] http://www.nai.com

[2] Wing, Stephen. "VBS viruses – Why and How Do They Spread So Quickly?" http://www.sans.org/infosecFAQ/malicious/VBS.htm

[3] Kerby, Fred. "Malicious Software (Malware) SANS LevelOne Security Essentials" 13th June2000 (25th July 2000)

[4] http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=W97M_MELISSA&Vsect=T

[5] http://www.officeupdate.microsoft.com/2000/downloaddetails/out2ksec.htm

[6] http://www.antivirus.com/products/trend_vcs/

[7] http://www.sans.org/newlook/digests/newsbites.htm

[8] http://www.antivirus.com/trendsetter/virus_report/

[9] http://www.zdnet.com/zdhelp/stories/main/0,5594,2289810,00.html

[10] http://www.zdnet.com/zdhelp/stories/main/0,5594,2684736,00.html

[11] http://vil.nai.com/vil/dispvirus.asp?virus_k=99011

Note, the cited security and virus newsletters and web sites are just a few of the many excellent sources of information about viruses and the vulnerabilities they exploit.

Appendix A

Below is an example of the standard message sent monthly to all employees at my corporation, depending on the most recent threats the wording might be changed slightly. However the basic content remains unchanged -

YOU are the first line of defense and some simple steps can prevent one of these new viruses spreading as quickly as the "loveletter" and "joke" viruses.

These latest viruses send e-mails using addresses from the address book in Outlook [and OWA], so it is quite possible that you might recognize the sender of the E-mail. The content is generally short and impersonal and will have a request to open the attachment - for example:

"kindly check the attached LOVELETTER coming from me."

"here you go "

"check this out"

Never open any unsolicited attachments - delete the e-mail immediately.

An unsolicited attachment would be one that you are not expecting - regardless of the origin. A legitimate attachment is one that you have requested from another user, or another user has told you that they are sending. Occasionally legitimate e-mails do have unsolicited attachments - a good example is the home office phone directory, in this case the e-mail will have sufficient content that will let you know exactly what is in the attachment.

If you are unsure of the "authenticity" of the e-mail delete it.

If you have questions call the virus response team at .....