

Virus Security for Small Enterprises

Chris Jackson 2001-02-28

Virus Security for Small Enterprises

by *Chris Jackson*

last updated Feb. 28, 2001

With the recent proliferation of .VBS exploits, virus protection for small enterprises has become increasingly important. After a recent outbreak of the VBS.plan virus at my company, I conducted a review of our procedures in order to upgrade our network's security against viruses. This article represents an analysis of a virus outbreak at a small my firm, including a breakdown of how the outbreak occurred, what conditions facilitated the outbreak and what could have been done to protect the firm against outbreak. It is hoped that this analysis will provide some insight into what other small to medium sized enterprises can do to avoid a similar fate.

Initial Outbreak

The company I work for is a small Internet firm that hosts its own DNS, mail, and IDS servers. Additionally, we have a significant number of remote users who have dial-up accounts from a national ISP. Our DNS server is an OpenBSD box running Bind, and our mail server is a FreeBSD box utilizing Postfix and PoP3d. Our IDS is a FreeBSD server running Snort. The majority of our users use Windows NT on their desktop and Windows 98 on their laptop. We have a few Mac users, as well as a few employees using FreeBSD. Our standard mail client is Outlook 2000, Eudora for the Mac, and mutt for the FreeBSD users.

We employ Norton Antivirus as our host-based protection and when a new virus definition update is issued, we post it on our internal file server and send a hyperlink to the file on Symantec's site to our remote users. Unfortunately, we don't have a system in place to ensure that all our users are updating their files. This led directly to our initial outbreak and to the subsequent secondary infection.

Apparently, one of our remote users became infected with the virus. Soon the virus, following previous .VBS examples, made MAPI calls to send itself out to everyone in his address book. We are uncertain whether he had failed to update his virus definitions, or if the latest virus update issued failed to include a definition for the VBS.plan virus. After the initial infection, two

workstations on our LAN were infected from the initial vector. At this point, the networking staff was notified, and we began sanitizing the victim's workstations according to instructions from Symantec's site. At the same time, we also notified both offices of the outbreak and sent out notices to our remote users. However, there was no plan or policy in place for situations such as this, and the ad hoc manner of our response was responsible for the outbreak persisting throughout the day.

In addition to the local infection, our IDS system notified us through e-mail that a possible .VBS virus was being sent out from our network. At this point we felt we had the situation under control, and sent an additional company-wide e-mail briefly explaining what had happened and trying to curb the amount of FUD generated by the outbreak.

Secondary Outbreak

Unfortunately, our optimism was misplaced. One of our users had disabled Norton on his desktop, as he felt it was inconvenient. This led to the second outbreak that breached our servers. This user had a mapped drive to a file server, and the virus used this to corrupt all the files of type .jpeg, .mpeg, .mp3, .jpg, .mp2, .js, and .css. Luckily, we were able to restore these files from tape backup with minimal difficulty. However, this could have caused considerable downtime had the virus carried a more destructive payload, such as the CIH virus.

Current Status

At this time, the majority of our users are now using an updated virus definition to protect their workstations against this particular virus. We can't be sure of our remote users, as we have no remote access to their laptops/workstations. Despite this infection, our company has taken no additional steps to change our operations or systems to prevent a future re-occurrence.

Primary Factors in the Outbreak

In general, the success of the virus in infecting computers on our network was due primarily to the following factors:

1. Inadequate virus definitions

Due to the nature of computer viruses, it is common that virus signatures are released only after considerable delay. Virus writers can test their creations against known anti-virus software

to verify their exploits. In addition, most viruses utilize Microsoft Visual Basic Scripting as the means of attacking hosts. Due to poor security implementations in most of Microsoft's e-mail clients, VBS has the ability to cause serious damage. Anti-virus software is, by nature, reactive. As a result, until vendors add new signatures to their update files, anti-virus software will be vulnerable to attacks by unknown viruses.

2. Disabled anti-virus software

With the freedom available to our users, each employee has the ability to disable virus software, as demonstrated in our outbreak. Additionally, each employee has the ability to install unapproved applications that may introduce security vulnerabilities or actual attack tools for compromising local hosts or hosts based on the Internet. Currently there is no Computer Use Policy in place to clearly define acceptable computer use. Nor do we have a management system in place to prevent users from using contraband applications. Such a policy would clearly state to users what changes to their computer's configurations would be acceptable, which would not, and why. This would mitigate the chances of an unaware user surreptitiously undermining the security measures that the system administrator may have put in place.

3. Poor user education regarding e-mail security

Most of our users are not computer security experts, nor do they need to be. However, minimal attention to fundamental security concerns is essential in preventing future virus problems from occurring. This requires that users be made aware of what factors may place a system at risk of infection, and what the user should or should not do. Many users blindly click on attachments they receive, a fact that is well known and well exploited by most virus authors. In addition, our users frequently circulate "cute" programs, which may very well contain Trojan programs. As e-mail is probably the most commonly-used application for most users, it is crucial that they be educated about proper, secure e-mail behaviour, such as not opening unexpected attachments and executable attachments. Users should also be apprised of the importance of updating their virus definitions.

4. Poor security focus in company - lack of a crisis plan

At the time of the initial outbreak, our company had no mechanism in place for notifying our employees of a virus incident, or security breach. Our ad hoc system consisted of each office notifying its members of the problem, and phone contact with our remote employees. Neither

proved satisfactory. If a comprehensive crisis plan had been in place, we might have been able to prevent the second outbreak. A crisis plan outlining the responsibilities of all personnel in case of infection or other security incident needs to be designed and implemented as part of an organization's broader security policy.

5. Additional vulnerabilities

In addition to being exposed to viruses through e-mail attachments, networks that are not solely Unix-based are also vulnerable to infection through embedded HTML, malicious Web sites, and ftp sites. Thus, security administrators should consider content filtering of all Internet traffic. Furthermore, in addition to these external threats, there is always the prospect of a virus being inserted into the network through some form of removable media. This could occur through negligence or malicious intent.

Once Bitten, Twice Shy - Avoiding Repeat Infection

Experience is said to be the best teacher. So how can systems administrators ensure that they learn their lesson from a virus outbreak? What changes can they implement to ensure that their system does not undergo a second outbreak?

1. Do nothing. Maintain the current system, and hope infection doesn't re-occur.

This is clearly not a rational response to a recent incident. Unfortunately, once the excitement of an infection wears off, the impetus for serious change is often diluted. Three important factors are political pressure, user convenience, and financial implications.

2. Strip attachments off at the mail server.

Stripping the attachments off of incoming mail would drastically reduce our risk exposure to the majority of today's viruses. However, viruses that are embedded in the body of an e-mail would still slip through this barrier. Embedded html exploits in e-mail might be caught by the virus software, but this again would depend upon up-to-date virus definitions.

Unfortunately, there are strong political implications of not accepting e-mail attachments, particularly if your company exchanges a lot of documentation with external organizations. The alternative would be to require users to FTP the files to a server, and then have the recipient

retrieve them. Users on the local network could simply copy their file to the appropriate shared folder. Unfortunately, this option would be unavailable for remote users.

3. Implement control software to monitor all computers.

Implementing Microsoft SMS or similar management software would allow a lockdown of all our workstations. This might be problematic for remote users, and would obviously work only with computers using Microsoft operating systems. In addition, SMS and programs like it are complex, expensive, and poorly suited for small enterprises. Also, the political implications of restricting users' freedoms shouldn't be underestimated: employees may feel that their autonomy is being unfairly restricted by the implementation of control software. That having been said, implemented in conjunction with the next two steps, this might be a workable solution, if not necessarily a palatable one.

4. Educate users about responsible computer use.

At first glance, this may appear to be the simplest solution, but it will not solve all our problems. For instance, employees at our company possess a wide range of computer expertise, without any real concentration in one department. A significant danger may be posed by the more experienced users who believe they know more than they do. This was a contributory factor in our second outbreak. Users who feels less comfortable with their computer are actually more manageable, as they do what they are instructed verbatim.

Nevertheless, computer training for all employees is a fundamental tool in addressing the problem. New employees should receive a basic computer orientation, bringing them up to a minimum level of competency that each organization should define in a comprehensive security policy. Education needs to be ongoing, as new threats and issues arise. A challenge facing our company in providing ongoing education is that our users are widely dispersed. However, despite the obstacles that any company may face, adequate user education is a vital step in limiting the chances of an outbreak.

5. Install a virus gateway scanner in front of the mail server

Many anti-virus manufacturers market software that sits on a mail server and filters e-mail for known viruses. Unfortunately, these programs are usually restricted in applicability to

Exchange, Notes, or, less frequently, Sendmail. However, some vendors also provide gateway software that sits on a separate server and scans SMTP, FTP, and HTTP traffic. It should be noted that traffic from HTTPS sites would not be scanned, however. At this time, there is no feasible option for scanning HTTPS traffic. While the expense of another server on the network may seem high, a virus gateway scanner may help to close three of the most prominent vectors for viruses. However, this solution will require a powerful server, as all your company's Internet traffic will traverse this box. When configuring such a server, be sure to determine whether the software is CPU bound, or I/O bound.

6. Install redundant IDS systems.

Our primary IDS system sits outside our firewall, and a secondary IDS system inside the LAN would prove valuable in early identification of infection. We utilize NAT on our firewall, so when the IDS caught the outgoing virus, it mapped to the single public IP associated with our LAN. If we had an additional IDS installed inside of our firewall, we could have pinpointed which hosts were infected instead of waiting for a user's cry for help.

7. Install relevant patches.

Microsoft has a patch for Outlook that forces the user to save an attachment before they can open it. While this additional step may give pause to some users, I feel that most would quickly become accustomed to it, and not gain any additional security. Based upon Microsoft's response to security concerns, I don't anticipate any significant enhancement in the near future. However, other manufacturers may offer patches to your particular client. Patches can strengthen inherent weaknesses that create vulnerabilities in software, thereby reducing one source of concern for security administrators. However, with this good news comes a word of caution: oftentimes, when users know that their system has been patched, they become less vigilant in practicing secure computer behaviours. While patches can strengthen security, they are no substitute for other security measures such as user education.

Conclusion

As a security topic, virus infections have often been relegated to second-class status. Many companies' feel that a firewall provides adequate protection against hackers and that host-based scanning software is like penicillin, a panacea against all viruses. Unfortunately, both of these assumptions are erroneous, as e-mail viruses represent a likely avenue for network

exploitation. The proliferation of e-mail clients that fail to adhere to common-sense security precautions will continue to provide fertile ground for those who wish to violate your company's network.

Despite most precautions, the more a company uses e-mail, the more likely it will eventually fall victim to a virus. Small enterprises have small budgets, and security is often an afterthought. While silver bullets are hard to come by, with attention, dogged determination, and careful analysis, you can dramatically limit your network's vulnerability.

Approach virus prevention as you would overall network security. Design a layered approach that protects your most valued resources first, and that allows for a modular, cohesive defence. Design and implement a crisis response plan, and tell your users what to expect in the case of an incident. Educating users is an integral part of protecting your users and your network.

Additionally, security administrators may want to plan how they will market these ideas to their management. I know that many systems administrators don't enjoy the political manoeuvring required to implement change, but unfortunately this is a necessity. The alternative is to allow someone less informed than you to impose inadequate security solutions. When those measures are breached, not only will you be asked to clean up the mess, but chances are good that you will be unfairly blamed.

Chris Jackson is a network administrator for a small Internet startup. He enjoys FreeBSD, home renovation, and spending time with his wife.

Relevant Links

[Symantec Security Update: VBS.Plan](#)
Symantec Antivirus Research Lab

[Protect Your Microsoft Office Data from Viruses](#)
Microsoft

[Fighting Computer Viruses](#)
Scientific American

[Eddy Willems' Free Anti-Virus Consultancy](#)
Eddy Willems

[Privacy Statement](#)

