Global Information Assurance Certification Paper

Protecting against mail viruses and worms: how to implement “defense in depth” in the security design?

GIAC Certification

GIAC Security Essentials Certification (GSEC)

Frederic RAIMBAULT

Practical v1.4b, Option 1

April 6, 2004

Abstract:

Mails containing viruses and worms have become a real persistent irritating problem in the first months of 2004. Each one of us has received several samples of these unexpected harmful messages in his electronic mailbox.
This is obviously not a new problem, but latest worms like Netsky, MyDoom or Bagle have used improved methods trying to jeopardize workstation and server security into many companies. Virus writers always discover new ways to propagate malware faster, passing through anti-virus and filtering software by hiding viral code and using some kind of social engineering to tempt users to click and execute attachments.
Network security has improved with network packet filtering and firewalls. Spreading techniques change regularly but mailing system is at the moment (with Web browsing http traffic) one of the most efficient methods to reach the weakest security area: the end-user and his desktop.
Several analysis show that in the last 3 years a huge number of companies suffered extensive virus infections and spent on average almost $100,000 to clean up each attack (source: CNET News.com [22]). The success of mass-mailers in early 2004 show that organizations are not making enough progress in defending against harmful code. Almost all of the companies surveyed said that at least 90 percent of their desktops have anti-virus protection, but still a third of the companies suffered virus disasters.
This document shows that there are efficient ways to implement security barriers at several levels, but the end-users must be effectively involved if we want to increase protection and prevent malicious software from reaching their targets. The level of their contribution will depend on the environment (Business mail, Home mail…), but the mailed worm is another typical security issue where “Defense in Depth” is needed.

1) How Electronic Mailing works:

There are two main tasks inside a mail server: The first one is the SMTP server (Simple Mail Transfer Protocol [1]) that handles the outgoing mails, and the second one is the POP3 server (Post Office Protocol [2]) that handles the incoming messages. POP3 can be replaced by IMAP (Internet Message Access Protocol [3]) that improves mail handling functionalities for the end-users.
Let’s take the SMTP / POP3 example. Figure 1 illustrates briefly how an e-mail message from Bob@ISP1.com gets to Karen@ISP2.com, assuming that they are connected to Internet through different Internet Service Providers (ISPs).

1) The e-mail client inside Bob’s computer communicates with the SMTP server inside the ISP1 mail server over the TCP port 25 [4] to send the message.
2) If the mail destination address is not in the same domain (ISP1.com), the SMTP server communicates with the Domain Name Server (DNS [5]) to gather the IP addresses needed to contact the SMTP server into the ISP2 domain. This information is stored in “MX records” into the DNS.
3) ISP1’s SMTP server sends the e-mail message to the ISP2’s SMTP server. The mail has reached the destination domain.
4) ISP2’s SMTP server recognizes that the destination e-mail address belongs to his own domain (ISP2.com). Therefore the ISP2’s POP3 server is able to store the message into Karen’s mailbox. Karen will be able to retrieve the message through POP3 protocol over TCP port 110 [4] next time she will connect to her mail server.

If for any reason the message cannot be delivered to the target domain's mailing system, it goes into a SendMail queue that will periodically try to resend it during a configured amount of time. If this process fails, or if the target mailbox does not exist, a "Delivery Failure" notification will be sent to the sender's e-mail address.

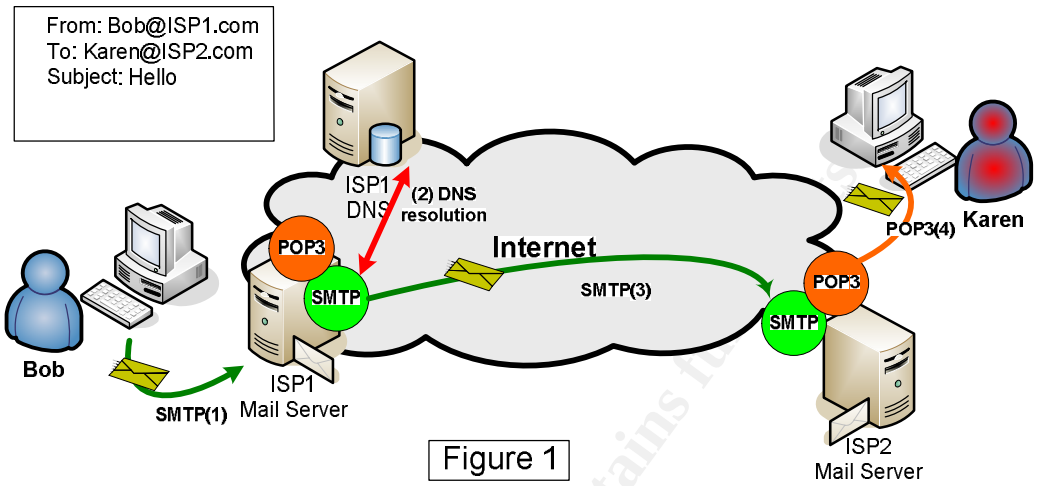


Figure 1

This simple example shows that e-mail messages are relayed by smtp servers through networks based on the domain name contained into the destination e-mail address ("To:Karen@ISP2.com"). It is easy to telnet to an SMTP server on TCP port 25, use the command-line shell to send an e-mail, and agree that the e-mail protocol is very basic. For instance, source e-mail address ("From:Bob@ISP1.com") is rarely checked.

Electronic mailing is so easy, and so cheap that many people take advantage of it to massively generate unsolicited commercial e-mails (Spam [10]) all over the world, reaching 50% of the total number of electronic messages at the end of 2003.

This is a first annoying problem since many companies are spending manpower and money to mitigate it and avoid the end-users to get disturbed.

The other problem is the multiplication of worms through the e-mail messages. The intent is to spread exponentially through the mailing systems by using several techniques, and damage server or desktop environments depending on the type of virus. Whether you are a "Home user" connected to the Internet through your ISP or connected to the network inside your company's intranet, this document describes solutions that can be put in place in both cases to try to lower the risks.

2) Description of the unwanted evil software:

Viruses are not new to computing environments, but the increasing use of e-mail and Internet connectivity added to the evolution of viral techniques have come to a point where everybody must recognize that this is a major security matter.

The escalation between Anti-Virus software and harmful code is a never-ending story. Bad workstation security and insufficient people training are certainly good reasons why mailing systems have been used by worms to propagate easily.

Those little pieces of code are able to install backdoors, launch Distributed Denial of Service attacks (DDoS), gather personal information, disable security tools, hide themselves into encrypted zip files or modify subject messages to bypass most of the detection softwares.

In the first months of 2004, several “famous” worms, like Bagle.x , Netsky.x or MyDoom.x have appeared causing troubles in many companies around the world Here is a brief description of one of them: Bagle.B (also know as Beagle.B)[7]

My name is Bagle.B …

Figure 2 shows how the infected message looks like:

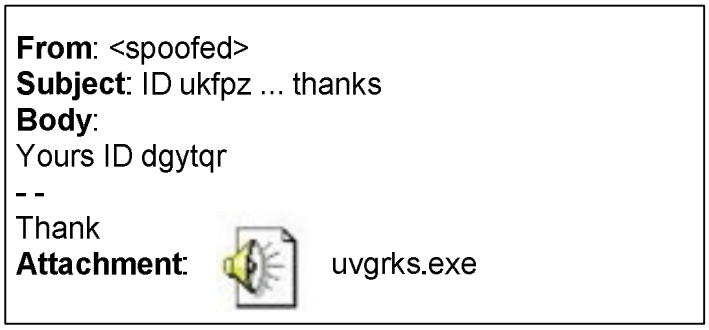


Figure 2

The source e-mail address (“From:…”) has been modified by the virus (spoofed). This message was not sent by the apparent sender. Nevertheless the presence of random characters into the subject, the body of the message and the attachment name could easily let you think that this is not a normal message. If this executable file is launched, here is the description of Bagle.B execution steps (from Symantec Security Response [7]):

1) The worm launches the Sound Recorder utility (sndrec32.exe).
2) It adds itself to the registry so it can be launched when Windows is started.
3) It opens a backdoor on TCP port 8866 allowing an attacker to upload and execute files to an infected computer.
4) It sends HTTP GET requests to the following Web sites on TCP port 80:
   www.strato.de
   www.47df.de
   www.intern.games-ring.de
5) It scans the local drives for e-mail addresses in files with the following extensions: .wab .txt .htm .html
6) It uses its own SMTP engine to send itself to all the e-mail addresses it finds.
And all this software is contained into an 11KB attachment…

3) Why Bagle.x and Netsky.x have passed through security protections?

With the first versions of the worms there were plenty of reasons to suspect that those messages could contain harmful code, and filters could be implemented quickly to stop them. It became much more difficult for detection tools to get rid of the latest variants because of their improved mechanisms, like many variations into the subject field, or attachment delivered into zip files. There have been twenty-two Bagle.x variants between Jan 18th and March 29th [8], eight variants of MyDoom.x between Jan 26th and March 03rd [8], and seventeen Netsky.x variants between Feb 16th and March 28th [8], each one with a different signature, with different goals and targets. Latest worms are hidden into an encrypted zip file, and the password is provided inside a pictogram into the message, passing through several security checkpoints

and getting into mailboxes. These are some of the reasons why virus detection updates have been available too slowly. The first detection mechanisms provided by Anti-virus vendors were not always optimal since they were based on basic rules like "any encrypted zip attachment with approximately an 11KB size will be quarantined". In addition, the delay between a new variant and the corresponding Anti-virus signature availability was each time a breach into corporate environments. Some of these vendors like Kaspersky [20] or Sophos [21] recently announced that they are able to detect password-protected versions of the Bagle worm at the e-mail gateway. Methods are still confidential since they are presented as a competitive advantage, and the accuracy will have to be verified in the coming weeks.
Finally, end-users are not running up-to-date Anti-virus Software on their desktops, do not follow basic security recommendations, and continue to execute suspicious attachments.

Open Mail Relays increase the problem:
There are a lot of poorly configured e-mail servers around the world that let anyone use them to send messages. Those open mail relays become channels for worms or spam and these systems are very helpful to attackers to hide themselves and to use these vulnerable systems' CPU to launch massive mail storms.
Most ISPs do not allow relaying of e-mail from untrusted domains, indeed just from any domains but their own. Many "Best Practices" have been documented, and several initiatives like DNSBL (DNS BlackList) [16], MAPS [17], or Spamhaus [18] maintain "well known non-secure" mail Relay Block Lists" (RBL). Those databases are used by many tools to stop messages coming from these mail systems. You certainly will not like to see your company's mail server in these blacklists. Before being removed from the database, a blacklisted system will have to be configured properly and tested.

4) What are the main annoyances and security issues for companies?

- Mail storms over mail servers and network bandwidth utilization.
- Mail spamming inside each person's mailbox.
- Lost of sensitive information.
- Backdoors installed on the infected workstations.
- Broadcasting of Business e-mail addresses over the Internet (that could potentially be used by spammers).
- By transiting through corporate SMTP mail servers and usurping business e-mail addresses, mail worms appear as if the company was the initiator of the message. This results in damaging company's reputation and customer relations.
- Programmed DDoS attacks against target Internet web sites are scheduled by worms, and will appear coming from infected companies through (authorized) "http get" requests.
- Costs of worm attack handling and virus damage repair actions
- Difficulties to detect malicious software into attachments without impacting normal messages.

I personally hate the fact that the sender source address is spoofed. My business e-mail address can be sent to plenty of people along with an infected message just because my mail address can be found in the address books of the persons that launch the virus attachment. The receiver of the next infected message will think that it comes from me, and there is nothing I can do to avoid that! (by the way, the amount

of “delivery failure” messages we receive show that many mails could probably be delivered…)

5) What defensive technical weapons can be used? Where should they be placed?

Many security tools and solutions are available to strengthen mail network design, based on the fact that preventive actions are taken to be in a better situation when the next worm attacks will happen.

Each company will put in place a solution according to its needs, and the decision will be based on several parameters like, for example:

- The number of employees to protect
- The money that can be spent for software and hardware
- The time and effort that can be put in place to manage the infrastructure
- The end-users technical competence and skills

There are several ways to build a secure mail infrastructure, depending on the level of protection. Figure 3 shows an intermediate Corporate Infrastructure overview.

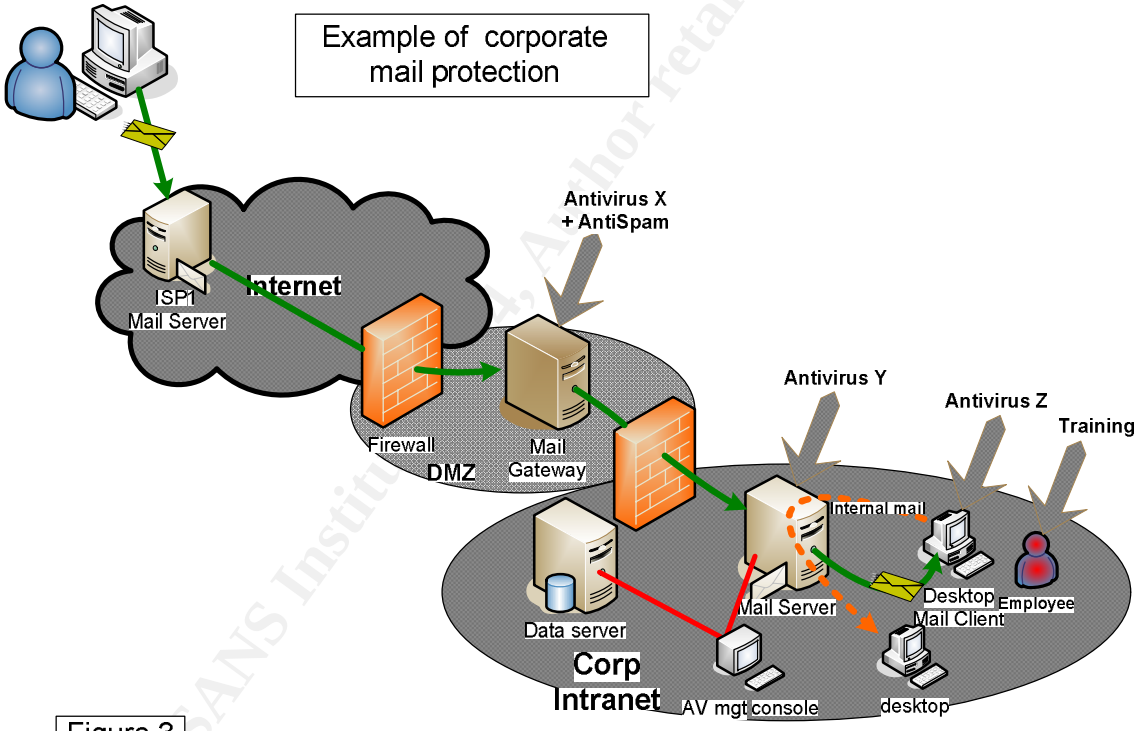


Figure 3

What can be done at Network level?

- An anti-spam solution can be put in place at the private network border, or the mail gateway. The main difficulty is to reach a good protection level without impacting normal mails. There are several commercial products like MailSweeper [6] or Trend Micro InterScan Messaging Security, and free products, like Spamassassin [12] that protect your network mail systems from spam and can be associated to an anti-virus program on the same system for more efficiency. In

general, these tools use several techniques like Bayesian filters (based on predefined word matching), Heuristics filters (analysis of the message structure), but also connection to RBL databases. More information on spam can be found in technical papers [10].

- Firewall rules must authorize only mail gateways to send or receive smtp traffic over the Internet. Employees should be obliged to use the safe corporate mail structure to send and receive messages. Firewalls should not allow any desktop inside the private network to send traffic on port 25 (SMTP) over the Internet, or to retrieve messages through direct connections on port 110 (POP3) to Internet mail servers. In addition, some companies have chosen to block all popular webmail sites as Hotmail, Yahoo, but this is a questionable decision. Implementing too many security filters can impact valid use of the Internet resources, and the result will be unhappy users trying to bypass the corporate policies.
- Reverse name resolution: This is the opposite of name resolution. Instead of asking the IP address for a specific domain (DNS) to route the message, the reverse name resolution mechanism looks for the domain name of a particular IP address. This is to verify the authenticity of the sender server. As shown in figure 4, the destination domain checks that the apparent source of the mail is valid before accepting the message. If the source IP address is different from the 3 Reverse MX records listed in the example, the message is blocked.

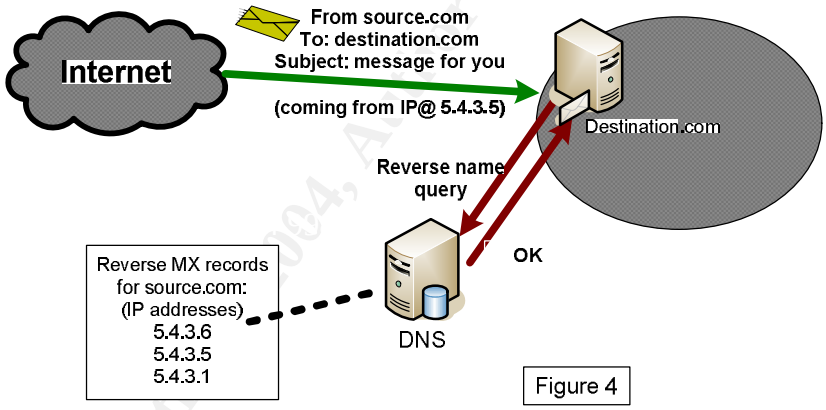


Figure 4

There are several drawbacks to this method. First problem is that the mechanism is based on DNS security. If the DNS can be compromised, the checking is invalid, or could lead to blocking of "good mails". The second problem is the additional DNS request: If the DNS is busy, this could slow down mail processing. The third drawback is related to Reverse MX records: if they are not well implemented, valid messages will be blocked. For these reasons, not all companies choose to implement it.

- Anti-virus software should be installed at different levels to increase security barriers. On the mailing path, the mail gateway, the mail servers, and each employee's desktop must be covered. They must be administered and updated immediately as new signatures become available. When new viruses arise, all vendors do not provide the product updates at the same time. They also do not use the same detection methods, therefore an interesting solution is to use different software vendors on different layers, and take benefits of crosschecking capabilities since they are serially traversed. In case of a new threat, the first available product update will protect you, and a little amount of time is

fundamental in these critical moments. The drawbacks are increased administrative and organizational efforts compared to a single vendor solution. This balance analysis must be done when selecting solutions. You could choose to put MailSweeper (or SpamAssassin) on the mail gateway, TrendMicro ScanMail [14] on the mail servers, and Symantec Norton Anti-Virus on the desktops. You can also think about installing the product that you think is best on the internal mail servers because they will be traversed by your internal mail flows…

- On the mail gateway, the security products are installed on the upstream side and will "offload" the mail servers by stopping the most important part of the unwanted messages. As shown in figure 3, with the "Corp" company network, the Corp mail gateway should block all inbound messages that have a source e-mail address like "aaa@Corp.com" since it would mean that the address of the sender is spoofed. This security element can also stop most dangerous file types or attachments with names containing double extension like "readme.txt.exe".
- A network sniffer (or a Network IDS) is very helpful to detect viruses when they are flowing through a private network because several pattern matching filters can be implemented to identify the virus spreading activity. With Nimda worm [9] in 2001, it was possible to detect the HTTP requests sent by infected computers, and isolate all compromised systems or desktops from the network.

What can be done at Server level (including Mail Server)?

- It is important to put in place an anti-virus structure that will be easily managed and updated. Most vendors provide products with centralized management of group configuration and reporting. It is then possible to concentrate alerts (quick detection), correlate events (isolate infected systems), and distribute new signatures throughout the network in a very short period of time. Several companies have implemented it for servers, but it would also be the right way to manage employee's workstations as well.
- Anti-virus software is mandatory, but not enough to protect from mailing threats. It is vital to perform content filtering at this level. Policy based security rules using combinations of both attachment verifications and mail content analysis must be integrated. Mail server products provide many built-in security capabilities for administrators. Both Lotus Domino and Microsoft Exchange solutions allow them to implement content checking on each message field, choose what attachments must be blocked (like .vbs, .bat, .exe, .pif or .scr), manage message queues, or isolate specific types of e-mails. Attachment detection can include "fingerprinting" (verification of the file type into the file itself, regardless of the apparent extension name). In case of virus alert, first initiatives should be taken at mail server level and at the mail gateway. Here is a case study example presented by Douglas Hitchen [23]
- Mail servers should not allow messages coming from any source. They can keep a list of all internal servers in the company that are authorized to send mail, and reject all messages coming from different sources that are by default untrusted.
- Perform regular health checking verifications. Among all the parameters that must be set properly, it is important to close all started daemons that are not needed (for instance Sendmail daemon on servers that have no need to send mails). Many of them are started by default on Unix systems. Hardening servers is the first way to protect them from being used as step stone relays to propagate malware.

- Apply patches! Missing security updates is the first thing hackers look at, taking advantage of security vulnerabilities to propagate malicious code . Having a patch distribution solution installed to maintain servers at latest software level in a timely manner is another way to lower risks.

What about Desktop level? (home or business desktops)

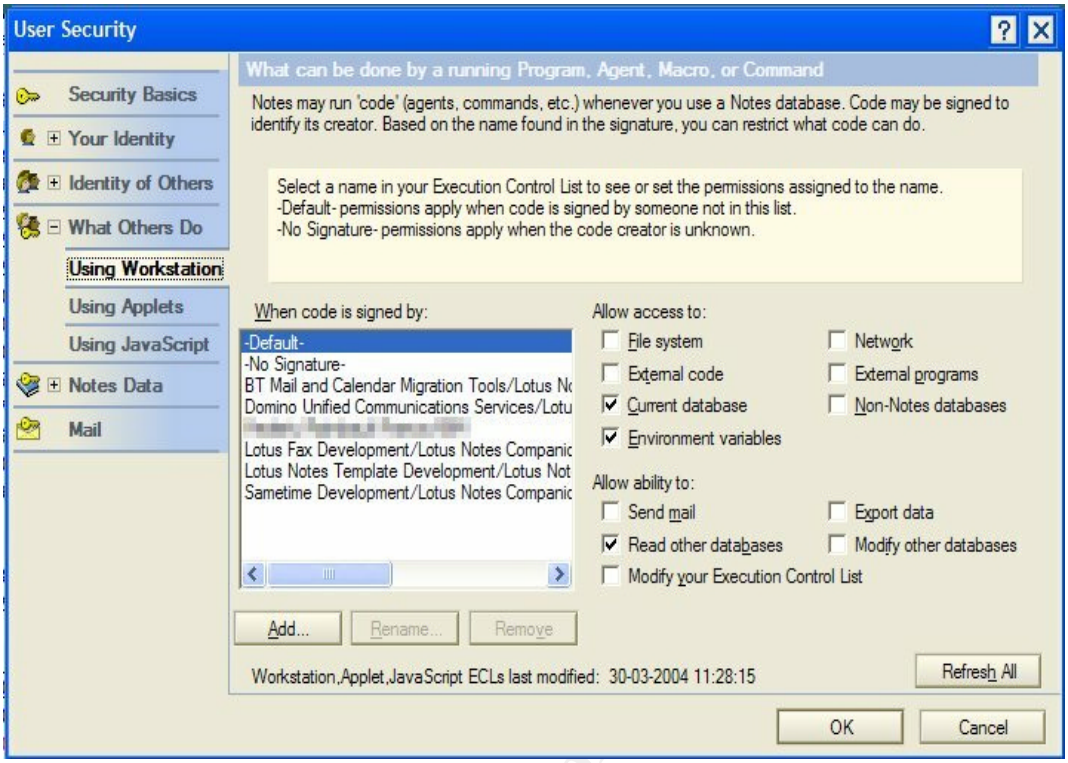
Desktops and laptops are more than simple endpoint systems. They contain a huge amount of sensitive information that is vital for company's business. They are distributed everywhere, mobile, moved outside the private network, used by many non-technical people, and not secured properly.

Here are "best practices" recommendations for securing end-users workstations:

- First of all, companies must have an enterprise anti-virus software license and put in place a simple way to automate installation and updates of virus signatures. Having a central administration of workstation anti-virus is a value-add. Signatures should be automatically updated on a daily basis, and a full system scan should be performed at least once a week. Home users can use free products like AVG (http://www.grisoft.com/us/us_dwnl_free.php)
- In business environments, an infrastructure should be in place to allow employees to backup their critical data periodically. More and more sensitive documents and mail databases are replicated locally to save space on Mail servers or lower costs, and a hard disk problem can always happen… more frequently than virus damage. Those companies sometimes provide employees with ready-to-use secured software builds for workstations.
- At operating system level, for a windows-based platform, it is important to:
  - Apply security patches frequently (windows update will have to become a routine) including application security updates (Internet Explorer, Outlook…).
  - Remove unneeded services (FTP server, Telnet, Web server) that are sometimes started by default, unless their use is justified. Those are additional possible proliferation channels for worms.
  - Disable the "Hide extensions for known file types" option. This possibility should be definitely removed from the Windows operating systems. It is useless and too dangerous when double extension file types are used in infected mails (readme.txt.exe would appear as readme.txt)
  - Disable windows script execution (The following tool allows you to switch it on or off, and it can be disabled in most cases) http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html
  - You should also use Microsoft Baseline Security Analyzer that helps to identify common security misconfigurations: (http://www.microsoft.com/technet/security/tools/mbsahome.mspx)
- Messaging software:

You can be using Lotus Notes client in a Corporate Lotus Domino infrastructure, Microsoft Outlook client in a Microsoft Exchange environment, Outlook Express at home, or any other Mail software. In all cases you must tune built-in security parameters.

For Lotus Notes, encrypt local mail databases, local database replications, and tune the Execution Controls Lists (ECL). The ECLs decide whether the signer of the code is allowed to have its code run on a given workstation. Here is a recommended settings example:



ECL must also be setup for Applets and JavaScript.

For Windows Outlook client, you should:

- Set the Internet Security Zone to “restricted zone” (disable all ActiveX options, disable Java, cookies, file download, scripts and more…). This setting removes many features, but there will be no operational impact on the vast majority of e-mail users since most messages are made of text and attachments.
- Enable attachment security (a first category is totally blocked, and a second category can be viewed by the user but not executed directly)
- Enable Macro security. You can choose to disable unsigned macros, prompt when a document contains macros, and choose your security level depending on your needs.
- Activate address book security. If code attempts to access your Outlook Address Book, a warning appears on the screen. You can either allow or block this access.

For Outlook Express (home users):

- Set the Internet Security Zone to “restricted zone”
- Enable “Not allow attachment to be saved or opened that could potentially contain a virus” checkbox
- Enable “warn me when other applications try so send mail as me” option.

Users can also implement basic filtering rules on their mail clients, and automatically classify or remove specific messages based on the content.

- Other security products can be used. They can be useful if an undetected harmful code tries to gather data or access the network.
  - Spyware/malware detection programs: They detect all suspicious code on your desktop. As an example Ad-aware is free for non-commercial use http://lavasoft.element5.com/software/adaware/ and has a signature liveupdate function.

- A personal firewall improves protection, and is absolutely mandatory on your home PC especially if you are connecting during long periods to the Internet for example through DSL connections. It will warn you if an unexpected software tries to access the network. Many products are available, and some of them are free like Sygate Personal Firewall http://smb.sygate.com/products/spf_standard.htm .

This is just an overview of the security topics that must be taken into account on your desktop, and you should look at them depending on the effort you are able to make.

6) What can be done at human and communication level?
Employee training:
As we said earlier, fighting against viruses is not exclusively a matter of technology. We saw that if software is not updated frequently, it becomes useless. All employees have different behaviors, and we are expecting them to react in the same way in similar situations. Everybody agrees that it is important to make security training of end-users, but this part of the security chain is almost never well implemented in companies. One reason is that those persons have different priorities, different technical knowledge, and many of them do not feel that the laptop is critical. They are using it like any electronic device, like a telephone. The laptop is just another tool they use to make their job. We can put in place more technical solutions, like central management of their anti-virus programs, remote installation of patches on their desktops; it will help a lot indeed. But it will always be important to make them understand a minimum set of "best practices" security actions and this will require a minimum effort from them.
Teach them the desktop security recommendations, including antivirus definition updates. Learn them why it is bad to forward a chain letter, and show them how to recognize one. We must explain them that Microsoft never sends e-mails all over the planet when a new vulnerability is found, but adds a security recommendation on the web site. End-users should be always suspicious when they receive unexpected messages and should not execute an attachment unless they know what it is.
P2P software like Kazaa or Emule must not be used inside companies since it can bypass most security walls and are often used to propagate suspicious software.
Effective and simple security communication must be put in place.
Another idea for non-technical users can be to show them how to secure their home computer with a simple and well explained cookbook. They may try to apply this at home and this could be the starting point of a security background.
Clear communication is important to the end-users, and they should know that the best virus-related information is located on the anti-virus vendor web site.

Incident management procedures must exist, must be tested, and must be maintained.
Worm infection will happen. It is very important to be prepared to this kind of event, and all the actors of this process should be trained to ensure that the right decisions will be taken quickly.
Mail system administrators, Network and Firewall engineers as well as Security contacts must be part of the process. They should know each other and be trained to work together in their day-to-day activities.

Several defensive actions should be listed as well as the parameters that must be analyzed to ensure a consistent and manageable handling of the incidents. This is important since those people can move to different jobs.
The process must describe the activation of temporary filters into Mail servers and also on the Mail gateway if it is part of the solution. Virus writers are creating new "features" each time, and it is very probable that the defensive actions will have to be improved. After a new incident, a quick verification should be performed to see if the virus incident procedure can be enhanced.
If the document is too general, it will not be used. It will not be updated, and will stay in a database for years.
The communication part is important and has to be included, but it does not mean that all people should receive a mail each ten minutes with the critical situation progress.
When do we have to inform end-users? Are we expecting something from them?
If a specific type of network traffic has to be blocked, this can have operational impacts on some of their activities.

Major Mailing security domains

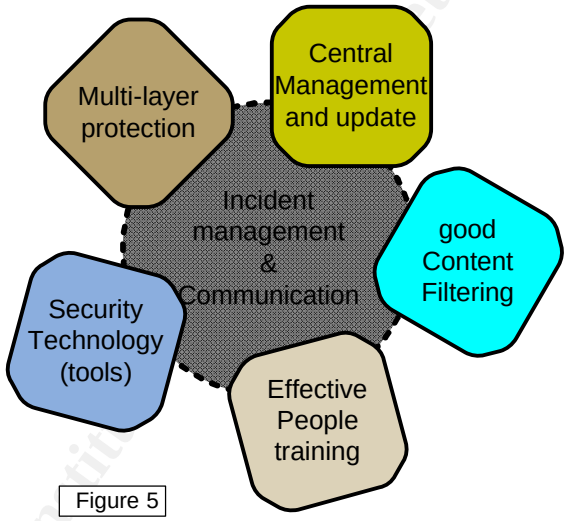


Figure 5

Conclusion:
Worms are taking advantage of the e-mail infrastructure to get to the end-users and take advantage of desktop security weaknesses. Several security parameters must be tuned on the desktops and the servers according to the business needs. It is difficult to find a good balance between security and end-user happiness, between blocking malware and allowing people to work.
For the moment, most of those worms are not highly destructive for the infected computer since they are mainly using them as a channel to propagate through the network. But what will happen if instead of just disabling security software they start to erase information on the hard disk or damage Bios on specific hardware types?
The "Witty" worm discovered by the end of March impacts only security servers and corrupts them by writing 65 KB of data to a random place on the drive. It began to spread only one day after the security software vulnerability was revealed!

As long as we will be using basic STMP protocol, mailing system will remain a potential risk. Authentication will have to be added one day to get rid of some of the problems like e-mail address spoofing.
Almost all companies are taking this security threat into account as a real Business security issue. But even if we are obliged to use several safeguards to protect the private network and corporate mailing system, there are several techniques that can be used to improve this protection like choosing at least two different anti-virus vendors, or implementing intelligent mail content filtering. But most companies do not have effective incident management procedures, and there will always be a risk during the timeframe between the virus birth and the availability of signature updates from the software vendors. For this reason, we must improve incident handling that will be part of this "defense in depth", we have to educate all employees with thorough training and make them understand that they are part of the security chain. Computer security is like car driving: Security is not the matter of others… it is everyone's responsibility, even if companies try to put in place security barriers.

References:

1. Klensin, J., "Simple Mail Transfer Protocol", April 2001, http://www.ietf.org/rfc/rfc2821.txt
2. Myers, J., "Post Office Protocol - Version 3", May 1996, http://www.ietf.org/rfc/rfc1939.txt
3. Crispin, M., "Internet Message Access Protocol", March 2003, http://www.ietf.org/rfc/rfc3501.txt
4. IANA.ORG, "Port Numbers", April 5, 2004, http://www.iana.org/assignments/port-numbers
5. DynDns.org, "How DNS Works", http://www.dyndns.org/support/kb/howdnsworks.html
6. ClearSwift, "MAILsweeper Business Suite", http://www.mimesweeper.com/products/msw/business_suite/default.aspx
7. Symantec Security Response,"Description of Beagle.b virus", http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.b@mm.html
8. Symantec Security Response, Virus Database, http://securityresponse.symantec.com/avcenter/vinfodb.html
9. Symantec Security Response, "Description of Nimda virus", http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html
10. Gburzynski, Pavel, "SFM: A Spam-Free Subscription-Based E-Mail Server", January 31, 2004, http://www.cs.ualberta.ca/~pawel/PAPERS/spam.pdf
11. Leyden, John, "Virus writers in malicious code hide-and-seek", March 5, 2004, http://www.theregister.co.uk/content/55/36049.html
12. Spamassassin, http://www.spamassassin.org/index.html
13. Grupe, Robert "Protecting Your Organization From Electronic Message Viruses" , June 4, 2001, http://www.securityfocus.com/infocus/1271
14. TrendMicro, http://www.trendmicro.com/en/products/email/overview.htm
15. Schmehl, Paul, "Holistic Enterprise Anti-Virus Protection", January 21, 2002, http://www.securityfocus.com/infocus/1538
16. DNS Providers Blacklists , http://www.dnsbl.org/
17. MAPS Real-Time Blackhole List, http://www.mail-abuse.org/rbl/
18. The Spamhaus project , http://www.spamhaus.org/

19. Microsoft, “Microsoft Baseline Security Analyzer V1.2”, February 20, 2004, http://www.microsoft.com/technet/security/tools/mbsahome.mspx
20. Kaspersky, “Viruses Can't Hide From Kaspersky”, http://www.kaspersky.com/news.html?id=146100010
21. Sophos, “Sophos protects against Bagle worm inside password-encrypted Zip files”, March 5, 2004 http://www.sophos.com/virusinfo/articles/baglezip.html
22. Lemos, Robert, CNET News.com, “Rise in virus attacks costs firms dearly”, March 19, 2004, http://news.com.com/2100-7349-5176420.html
23. GSEC - SANS Security Essentials Certified Practicals , http://www.giac.org/GSEC.php

- Hitchen, Douglas, “Case Study: Spam Blocking, Content Filtering, Virus Scanning and Attachment Blocking in a Novell GroupWise Environment With Guinevere, SpamAssassin and Symantec (Norton) Anti-Virus Corporate Edition”, September 2003, http://www.giac.org/practical/GSEC/Douglas_Hitchen_GSEC.pdf

(All URLs verified on April 6th, 2004.)