Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Detecting and Recovering from a Virus Incident

There is an ongoing battle between the creators of computer viruses and malicious code and the firms creating software to prevent their actions. While antivirus firms are adding proactive technology to their software, when it comes to new types of viruses, they still largely depend on reacting to the actions of the virus creators. Short of dismantling your network, there is no way to totally protect your environment from the next new fast-spreading virus. This document lays out what information to gather and the steps ...

Copyright SANS Institute
Author Retains Full Rights

AD

GSEC Practical Assignment Version 1.4b Option 1

Detecting and Recovering from a Virus Incident

John Stone
November 15, 2002

Introduction

There is an ongoing battle between the creators of computer viruses and malicious code and the firms creating software to prevent their actions. While antivirus firms are adding proactive technology to their software, when it comes to new types of viruses, they still largely depend on reacting to the actions of the virus creators. Short of dismantling your network, there is no way to totally protect your environment from the next new fast-spreading virus.

This document lays out what information to gather and the steps to take in the event malicious code enters your environment. It assumes that you may not have in place all the tools or infrastructure necessary to deal with the intrusion effectively. It explains how to detect a virus if you are infected, what immediate response you should make, the stopgap measures you should put in place, how to approach the task of environment cleanup, and some long-term solutions. In this document, we will call all malicious code a virus, even though that term may be technically inaccurate in some circumstances.

Identify the attack

Recently email has been the primary method of the virus distribution, but it is not the only method. The other ways a virus can enter your network environment includes floppy disks, FTP downloads, and HTTP downloads, among others. Most recently virus writers and intrusion experts have been cooperating and developing viral code that enters networks by exploiting known security bugs.

Once a virus is within your network, it can spread from computer to computer in multiple ways. Some viruses will search the network for systems with active shares and try to access them. If possible they will infect a file on the accessed system. Other viruses will email themselves to others in your environment and thus attempt to infect their computers. Some will do both. Others can spread in completely different unexpected ways, including the use of instant messaging systems or peer-to-peer applications. The result is that it can only take one infected computer in your network to infect many other systems in the environment.

Detecting the infection

In many cases the discussion surrounding the detection of virus infections centers on the activity of antivirus software. What is often overlooked is that if antivirus software can detect an infection or an infection attempt, it can usually deal with the situation effectively. A virus incident will only occur in situations

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

where the antivirus software was not able to detect the infecting agent, at least not initially.

There are several types of indicators for possible infection. Indicators can result directly from a specific virus payload, as a side affect of the virus payload, or as a result of the virus's attempt to spread. Indicators of virus infection include:

- Interface indicators include audio sounds or screen images that appear unexpectedly, especially if the same audio or images appear on multiple systems. The sounds or images are a payload of the virus. While the indicators are non-destructive, this does not mean the virus is not destructive. Since users are always presented with seemingly random audio and images these indicators are easily overlooked unless they are obtrusive. You must depend on your users to detect this type of indicator; user education is key in this area.
- File indicators are the most common but often the hardest to detect. They include the appearance of multiple unknown files on workstation or on file servers, the disappearance of multiple files for unknown reasons, the loss of data within data files, or the replacement of file contents. If the virus is a file infector, another indicator is the changing of file size on files that contain executable code, as the virus inserts itself into the executable code of the file so that the virus executes when a user or application attempts to run the code in the original file. Often you discover these indicators as the result of user notification but the best way to detect this type of indicator is through some sort of host-based intrusion detection solution.
- System indicators are usually easy to detect as they often interfere with the ability to use the system. They include file partitions becoming unavailable or the destruction of complete file systems. This type of damage is rare as it interferes with the ability of the virus to spread. When this does happen, it is often the side affect of poor programming on the part of the virus creator but can be the result of a logic bomb put in place by the creator to execute based on a trigger, such as executing on a specific date. Your users will always let you know about this type of indicator.
- Network indicators are usually caused by the side affects of the virus attempting to spread and include network storms and unscheduled email outages. This type of indicator is usually obvious to many users at the same time but can also be detected through the use of network administrative tools with notification capabilities.
- Custom indicators are ones that you put in place in your environment specifically for detecting new viruses not detected by antivirus software. An example of a custom indicator is putting in place a dummy Microsoft Exchange email group list account including only dummy user accounts in order to detect email worms that use Microsoft Outlook to spread.

While many indicators of a virus infection can be easily tracked to a specific action or a specific trigger, in some cases the indicator can occur at random

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

times that can not be reliably predicted. These are the hardest to track down and determine if they are in fact caused by a virus intrusion into the environment.

Initial research

It is important to note that all of these indicators can occur for reasons not virus related and one of the first tasks is to determine the source of the indicator. Non-viral causes of virus indicators can include joke programs, advertisement messages, application errors, common user mistakes, system failures, and network hardware failures.

When attempting to determine the cause of the virus indicator, it is important to perform some research on both known viral and non-viral issues that could cause the same indicators.

Consider the following sources:

- Virus Protection software vendors, such as Trend Micro (www.antivirus.com), Sophos (www.sophos.com), McAfee (www.mcafee.com), and Symantec (www.sarc.com)
- The Computer Emergency Response Team (CERT) Web site: www.cert.org
- The ICAT Metabase: icat.nist.gov
- The System Administration Network and Security Institute (SANS) home page: www.sans.org
- The NTBugTrack Web site, which maintains a database of known application issues: www.ntbugtrac.com
- Operating system-specific sites including Microsoft (www.microsoft.com) and Sun (www.sun.com)
- Application-specific sites for the software used in your environment
- Hardware-specific sites for those systems affected
- The Computer Virus Myths Web site, which maintains a database of known virus hoaxes and common application issues mistaken for viruses: www.vmyths.com

Identify the infector

Once you have determined that the cause of the virus indicators is in fact a virus threat, you need to identify the nature of the attack.

- Determine the target operating systems since most viruses affect only a limited set of platforms.
- Learn how the systems are attacked, such as which ports are used.
- Gather process information from infected systems using tools such as handle.exe, listdlls.exe, and pslist.exe available from Sysinternals at www.sysinternals.com, fport.exe available from Foundstone at www.foundstone.com, and the native netstat.exe program on Windows 2000 systems.[1]
- Assess commonalities between the affected systems.

[1] Carvey

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Discover virus payloads such as deleted, renamed, or newly created files, changing of file attributes, deleted, changed, or newly created configuration information, or changes within shared library files.

Assess issue scope

Performing a full inventory of your environment to determine the total impact of the virus on the environment while possible is not the most efficient method of determining your exposure to the virus threat. In some cases the virus will spread faster than you can assess its spread. It is still possible to make an educated guess concerning the scope of the issue.

Assess the infection vector:

- How does it arrive in an environment?
- Is it network aware and propagates via shares?
- Does it use groupware or email gateways to further propagate?
- Does it enter the environment through security holes?

Determining this information will help you create the fastest method to stop its spread.

Assess spread of infection:

- Investigate administrative and high availability computers that are currently infected.
- If the virus is network aware, is a network administrator account compromised?

Determining this information will help you determine which computers in your environment are likely infected.

Coordinate the response

After you have identified the attack, you must gather the proper team to deal with the threat. This team is responsible for determining options, recommending the proper solution, and implementing the solution decided upon. If you already have in place an incident response team and incident response procedures, you should use this infrastructure to deal with the virus threat.

Call in the reserves

If you determine actions other than updating your antivirus software and virus signatures are required to clean your environment, this is the time to call in a team to assist in the project. This team will need to assess the scope of the issue, create a plan to remove the virus, and then execute the plan. The size and makeup of this team will depend on the level of infection distribution in your environment. This team should have a designated team leader responsible for driving through the process of resolving the virus infestation issue. Teams involved in the response process should include the following:

- The help desk will receive calls from users complaining about the indicators of viruses. They are often the department that raises the initial

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

alarm. They can be involved in communicating the response processes to employees.

- If an incident response team exists, it should be the coordinating agent, researching the specifics of the virus, recommended responses, and initial infection points.
- Workstation operations and server operations teams are involved in tracking down infected systems, identifying high priority protection points, and communicating the response processes. Both teams may need to patch systems as part of the response process.
- Network communications may end up blocking connections at the perimeter or segmenting the network to contain the spread of the virus. They should audit firewall and router logs for indicators of initial infection points.
- The messaging team may be called upon to down the email servers, reconfigure the email servers, or patch the servers as part of the response process. They should audit email logs for indicators of initial infection points.
- A legal representative may be called upon to assist in forensics investigation activities after containment of the virus and can provide guidance on when this is necessary.
- An accounting representative may be required to determine the financial impact of a virus incident to assist in determining the necessity of an investigation.
- Public Relations staff may be required if the virus incident or the response processes is of high enough impact it will cause a noticeable impact to productivity or when the virus has spread from your network environment to business partners, customers, or others.
- If it is found that a virus incident resulted from an employee or contractor violating policy, a representative from Human Resources may be required.
- A management representative is required in order to make decisions on responses that can negatively impact productivity and on investigative action. The incident response manager will have to work closely with management to determine their authority.
- Representatives of departments directly affected by the incident.
- As part of the recovery effort you may even wish to bring in external assistance.

Clear communication paths between teams is absolutely necessary in order to properly coordinate activities to determine the cause of the virus infection, the initial infection points, the spread of the infection, and the proper response. As you begin the response process, you need to determine how to communicate the problem to all the teams, how to escalate the problem properly, how to track solution progress, and when to bring in each team into the response process.

Virus incident command center

If financially feasible, every company should have available a command center to use in responding to any security incident, including recovering from a virus

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

incident. It allows you to efficiently work through the process of identifying the problem and solutions and coordinate the response. With a command center you can properly control virus incident communication. A command center will reduce response time, coordinate information, direct containment activities, perform virus research, receive instructions from antivirus vendors, and receive operational instruction from management.

Proper setup of a command center

In order for a command center or any response location to function properly in reacting to a virus incident, a few items are required:

- Rapid access to representatives of all teams directly involved in the response process.
- A list of all key players to inform concerning a virus incident and status updates.
- A list of additional individuals to contact in case the problem escalates.
- Contact information for legal, accounting, public relations, and management.
- Contact information for business partners as they could also be at risk from your virus incident or the initial cause of the incident.
- Dedicated telephone lines and functional telephone equipment connected to those lines. As many current business telephone systems are computer operated and thus possibly affected by either the virus incident or the response processes, it is imperative that a backup communication method is also available, such as cellular telephones.
- Fully functional network connectivity with dedicated LAN lines.
- Access to central management software for all installed antivirus and intrusion detection systems.

In addition, a true command center should also have the following:

- Tested two-way radio communication for the local campus in order to keep the phone lines free for remote site communication.
- A functional CD burner that is used for creating CD's when it is necessary to distribute software patches and updated virus definitions.
- A dedicated power supply for the building housing the command center or for the command center room itself, with a backup power source also available.
- Computer systems with all current antivirus and content filtering software installed in the environment. These systems should be tested to be virus free.
- Segment connectivity of the command center from the internal network in order to provide a level of protection against virus infection.
- Segment connectivity to the Internet, bypassing the internal network, so that the command center can access Internet resources when the proper response to virus incident is to disconnect the internal network from the Internet.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Proper use of a command center

Not every virus incident will require the use of the command center. Examples of when to use the command center includes when a virus worm is spreading fast through email or through the network environment, when a virus incident is adversely affecting productivity for a significant portion of the environment, and when you expect containment and cleanup will take longer than a day. It is also a good idea to make use of the command center and include your business partners in the process when you are aware that the virus incident has spread or could spread from your environment to theirs.

When you first enter the command center, perform the following steps:

1. Contact upper management and inform them of the emergency.
2. Contact all key players and invite them to assist if it is necessary or promise to keep them informed if not. Provide your location information and obtain theirs in order to ensure continued communication availability.
3. Test the command center to validate that all elements work correctly such as phone and network connectivity.

Recover from the attack

You must locate all systems that are infected and clean each of them completely in order to regain control of your network. In many cases this is a lot easier to say than it is to do.

Immediate response

There are some basic steps you should take whenever you suspect your environment has become infected with a new virus.

Update your antivirus software

Assuming you have antivirus software installed in your environment, the first thing to do is determine whether your antivirus vendor has released an update that will detect the infection. Hopefully they will also have a repair methodology available. It is best to let the experts, whenever possible, determine the best method of removing a virus from systems and networks.

When a new virus infects your environment, the most important response is to install all updates to your antivirus software that are necessary to detect and repair the virus. Follow these steps:

1. Obtain the detection signature for the virus from your antivirus vendor.
2. Obtain a technical description of the virus from your antivirus vendor.
3. Test the detection signature update provided by your vendor in your virus signatures staging lab.
4. Distribute the fix to your environment; using whatever method you have in place for rapid deployment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Make sure all antivirus services on workstations, servers, email groupware servers, SMTP servers, and content filtering Firewall proxy servers are updated as well; this will help prevent the spread of the virus through those vectors.

Educate yourself

If your environment is infected with a virus, it is important to understand what the possible repercussions are to your environment. Educate yourself on how the virus spreads, its method of attack, and the possible damage it can create. It is possible that updating your antivirus software virus signatures is not sufficient action to clean your environment from the virus.

It is not necessary to depend solely on your vendor for information on the virus. Other vendors and news sites will also usually have information available; however, you might find conflicting information. If such conflicts occur, you should contact your antivirus vendor for clarification.

Consider the following sources:

- Virus Protection software vendors, such as Trend Micro (www.antivirus.com), Sophos (www.sophos.com), McAfee (www.mcafee.com), and Symantec (www.sarc.com)
- The Computer Emergency Response Team (CERT) web site: www.cert.org
- Major news web sites including CNN (www.cnn.com) and MSN (www.msn.com)
- The Virus Bulletins web site: www.virusbtn.com
- The International Security Industry Association web site: www.icsalabs.com/html/communities/antivirus/index.shtml
- The Computer Incident Advisory Capability web site: www.ciac.org/ciac
- The Information Systems Security Professionals portal web site: www.infosyssec.net/
- The National Institute of Standards and Technology: csrc.ncsl.nist.gov/virus/
- Security Focus: www.securityfocus.com

Submit a sample file

In the event that the latest virus signatures do not detect the infection, you will want to submit a sample for analysis and signature creation. Usually the submission of a sample file is a straightforward process as the virus was detected and stopped but the antivirus software was unable to repair. In this case the antivirus software itself can perform the task of obtaining the sample. In the case of a new virus strain, it is up to you to locate a sample. While it is true that your vendor will most likely obtain a sample eventually, it is also possible that you were the first victim and might be the only victim thus it is imperative that you obtain a sample for your vendor.

It is also imperative that the sample be obtained correctly. Thus, you should contact your antivirus vendor's technical support line for assistance on this task.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Eradicate the threat

In some cases, it is not sufficient to just update your antivirus definitions and scan your systems to remove the virus from your environment and in other cases, some infected systems in your environment may not have antivirus software installed. In these cases, it is necessary to take extra steps to remove the virus completely from your environment.

You must formulate a plan to respond to the problem, ensure all parties are satisfied with the course of action, and execute the plan.

Stopgap measures

Discovering all the infected systems and eradicating the virus on those systems will often take some time so it is important to determine what steps you should take while waiting for the process to complete in order to contain the continuing threat.

Base containment steps on your incident response policy, if it exists, and only after you have gathered sufficient information to make an educated decision and have obtained approval of management for each step. The containment plan should include when the stopgap measures are backed out returning normal functionality.

All containment activities should be controlled centrally after coordination with all affected parties. In order to determine which parties are affected, it is necessary to determine the resources affected and the importance of those assets. These may include messaging servers, Web servers, Internet access, file and print servers, or application servers. In some cases, it may be easier to determine the parties affected based on departmental division or location.

If the virus can spread through email, concentrate on updating the protection on your email groupware servers and SMTP email gateway servers first; these are the fastest means of spreading the infection internally and externally.

If the virus can spread through HTTP or FTP access, concentrate on updating the protection on your filtering proxy servers.

If the infection is spreading faster than you can distribute the fix, you will want to consider disabling services allowing incoming requests to contain the attack. This is especially important in the following situations:

- When antivirus signatures are not yet available from the vendor.
- Content filtering is not possible due to changing content.
- Users are not properly educated concerning the virus threat and their role in protection.

Refer to the technical write-ups on the virus, if these are available, when considering containment actions. Actions to consider for containing the attack include:

- Partition the network using firewalls, routers, or switches.
- Reconfigure DNS to disable incoming SMTP email.
- Change content filtering software to block all email attachments.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Change content filtering software to block email containing certain strings of text.
- Block Internet HTTP or FTP access.
- Send users home in departments affected by the outage.
- Remove workstations from the network, allowing users to continue work locally.
- You may also want to write-protect critical data areas that are accessible to the virus on high priority systems.
- Create dummy files on non-infected systems that will prevent infection of the system.
- If the risk is extremely high, you may find it necessary to completely disconnect the network from the Internet.

You should also disable services providing outbound requests in order to protect your business partners, customers, and other corporations. This may include disabling outbound email or certain ports at your firewall.

Identify infected systems

It is important to discover all the systems infected by the attack, as you must eliminate all sources of infection in the environment or else reinfection of other systems can occur. You should start by trying to establish system zero(s), which were the first systems attacked; it is then easier to determine which systems or services to deactivate. Consider the following strategies to find system zero:

- Use network traffic analysis applications to track the spread of the infection.
- Compare system files between systems to determine the path of infection by determining when files were created or changed. The earlier the timestamp on the file the more likely it is that the system was infected first and then spread to other systems.
- If available, compare file system status against file and directory footprints.
- Check the log files of perimeter systems and messaging servers to determine ports that are unusually busy.
- Identify new servers in the environment, as they are often system zero due to inefficient patching.
- Check the status and log files of forward facing systems to the Internet including gateway and messaging servers.
- Identify new workstations placed on the network, as they are often carriers of viruses into the environment.
- Check the log files of VPN servers to determine if there is a correspondence between the initial infection point and a VPN connection.
- Determine who first reported the attack and query them for more information.
- Determine the typical system attacked in order to create a profile of the virus you can use in searches. This might allow you to identify system patches you can distribute or services you can turn off to mitigate the affects of the virus.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Do not forget to check with additional parties that may affect your environment such as business partners and temporary contractors or employees. At the same time you should also determine if there is a danger of infecting partners.

Environment cleanup

Cleaning up damage from a severe virus infestation can take weeks in a large enterprise environment. It is therefore important to establish a clear and concise cleanup procedure with the input from all teams that are involved in the process. These teams will include the help desk, messaging, Web server administrators, server operations, workstation operations, and others. You must then effectively communicate that procedure to all teams involved.

When creating the cleanup procedures, you must consider the following:

- For all viruses, you want to obtain and distribute to all systems updated virus signatures that detect the virus and repair it if possible.
- For certain viruses, there may be a removal tool created for computers already infected. If so, that will need to be distributed as well.
- If a tool does not exist, but removal instructions are available in the virus technical write-up, you either need to develop a script to accomplish those directives or manually run them.
- In any event, the antivirus software should remove the malicious code itself once the updated virus signatures are delivered.
- You might require a completely different process for systems that do not have antivirus software installed. In most cases, it is advisable to remove the virus from the system before installing the antivirus software.
- Recovering systems using stored system images may be more cost effective.
- Availability of backup servers is required to ensure quick repairs of altered files.

In general the cleanup process will follow these steps:

1. Obtain the detection signature and any required fix tools for the virus from your antivirus vendor.
2. Test the fix provided by your vendor for the virus in your virus signatures staging lab. This may include separate repair tools that you need to run before using the updated virus signatures.
3. Develop a deployment methodology for the fix process.
4. Create a cleanup plan and validate with all affected teams and your antivirus vendor.
5. Clean all infected perimeter and email servers and update the virus signatures of the antivirus software providing protection of these avenues of infection.
6. Distribute the fix to all the workstations and servers in your environment using whatever method you have in place for rapid deployment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7. Isolate systems that are infected and require repair.
8. Run all required fix tools on all infected systems in order to remove the virus from memory or disable it.
9. Scan all systems with the updated virus signatures to remove all infected files.
10. Eliminate all temporary and suspicious files, including hidden directories and files.
11. Remove or alter configuration information used for the functionality of the virus or that might allow the virus to reappear.
12. Remove configuration information that may cause system failures.
13. Search for newly mounted partitions created by the virus and eliminate them.
14. Search for missing log partitions and restore.
15. Search for added or altered user accounts and remove or restore.
16. Restore changed or deleted files.
17. Distribute patch updates to all systems and update patch levels.

To ensure the project is completed successfully, it is necessary to check in with the individuals performing the cleanup and continually track their progress. Consider the following points when tracking progress of the cleanup project:

- Conduct spot checks of the cleanup process to assure that proper procedures are followed.
- Use written forms to track progress to ensure all systems are cleaned or patched.
- Use the help desk to lead the cleanup project utilizing on-site IT personnel to perform the actual clean-up duties.
- Have two separate teams monitoring progress to ensure the work is accomplished correctly. Use teams familiar with incident management such as virus management and vulnerability management teams.[2]

Investigate the cause

There are two reasons for investigating the cause of a virus infestation attack. One reason is to gain an understanding of what vulnerabilities were exploited so that you can mitigate the risk in the future. The end result of any forensics investigation is a lot of information you can use to increase your level of security against virus intrusions.

Another important reason is to gather evidence for possible civil or legal prosecution. Evidence can include files changed or left behind by the virus. It is necessary to assume that civil or legal prosecution will occur until decided otherwise. You must take the proper steps to secure the evidence before it is lost or becomes legally tainted.

[2] Symantec Corporation

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Forensic activities start during the recovery phases of the process. After a virus infestation, there are usually many systems you can choose from to set aside for forensic purposes. It is best to set aside a system identified as system zero as it may contain evidence not present on systems infected later in the spread of the virus. Use the following recommendations when securing the selected system for further forensic investigation:

- Do make changes to the system unless otherwise directed or have a specific purpose.
- Ensure that normal operation of the system does not overwrite data. If possible, disconnect the system from the network, down the system if necessary, and turn it off.
- If it is not possible to disable the system, backup key system files including configuration files, registry files, and logs.

One of the first things to determine is if the attack was targeted at your environment and if so were internal employees or former employees involved in the attack. Based on this determination, you may then decide to perform in depth computer forensics. Computer forensics requires specific expertise.

> *A forensic expert will extract the needed information from the compromised system(s) without altering the original data. In order to interpret the degree to which malicious activity has occurred and to understand the extent of the incurred damage, the forensic investigation is dependent upon the preservation of the information.*[3]

It may not make sense to perform in depth forensics activity yourself if you at all suspect involvement of internal staff or the possible loss of data confidentiality. Contact an expert instead.

Implement solutions

Do not gamble with the security of your network. To effectively protect your environment against a virus intrusion, act proactively to address the weaknesses in your policy foundation and the security point solutions you have implemented to assist in enforcing the policy. After a virus incident, it is important to revisit your policy and technical infrastructure in order to determine where you can make changes that will provide you a higher level of security and, hopefully, mitigate the affects of the next incident.

Policies form the basis from which the security of your environment flows. A policy foundation includes high-level goals, standards to use in meeting those goals, and processes used in meeting the standards. The first step in implementing any solution is to assess the status of the current policy infrastructure to determine where changes are required. Policy changes to consider include:

- Update the written policies to address the new threats including requiring proactive centralized intrusion notification solutions, content filtering of

[3] Osborne

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

email, Internet, and network traffic, and blocking of high risk Internet resources.

- Include enforcement as the part of policy. You can implement the enforcement through the use of technological solutions or through the setting of clearly stated ramifications if the policies are not followed.
- Create incident response procedures and a put in place a Virus Response Team. Provide all users with a single point of contact into the incident response processes.
- Clarify or adjust the reporting structure within the technology departments to simplify the response processes.
- Institute communication processes between teams to also assist with the response processes.
- Put in place a training program for all users to educate them on the danger posed by viruses and their role in prevention.
- Educate upper management on the importance of providing proactive protection from viruses.
- Require that all critical files be stored on servers for backup purposes.

Once the policy infrastructure is updated, it may be necessary to update the technology infrastructure in order to implement the policies effectively. This may include the following:

- Install antivirus solutions throughout environment to provide filtering of email traffic, Internet traffic, network traffic, and local file access.
- Implement a central management model for the antivirus software to allow for a higher level of control over the software configuration and level of currency of the virus signatures.
- Installation of both host-based and network-based intrusion detection technology. Host-based intrusion detection provides the ability to detect virus infestations missed by antivirus software. Network-based intrusion detection technology assists in the effort to determine the spread of the infection.
- Install Security Management software to monitor policy adherence, including the patching of systems.
- Simplify the network topology so it is possible to segment the network to provide enclaves during a virus infestation.
- Install email content filtering technology that can block email based on strings of text in the subject line or the body of the message.
- Implement an internal Instant Messaging solution so that users do not have to use an externally controlled solution.
- Implement desktop firewall software to provide the ability to block the spread of a virus through specific ports. A desktop firewall solution is especially important with the advent of VPN and wireless network solutions.

Any updates to the policy and technology will require changes to administrative processes. Points to consider include:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Hiring of a full-time antivirus administrator. For many medium-size companies or larger, virus management is a full-time job. Investigate the possibility of outsourcing this asset to security partner.
- Investigate outsourcing of security management of a subset of the environment to managed system security providers. This is especially effective for perimeter devices.
- Institute routine backup processes and monitor compliance. An aggressive backup schedule is imperative to assure the minimum loss of data in the case of an extreme virus infestation event.
- Prevent users from disabling antivirus software.
- Limit the allowable file extensions for email attachments.
- Put in place a process to keep system patches up to date.
- Institute technology or processes to verify antivirus software is running and up-to-date.
- Lock down workstations so regular users have limited ability to modify their systems including configuration and system files.
- Disable the Windows Scripting Host as it is not often needed by users and provides a known propagation method. You may also want to remove scripting in Outlook and Internet Explorer.[4]
- Disable the ability to access external instant messaging systems, news groups, email servers, or other externally controlled communication platforms.

Each virus infestation event will always differ from the last but with some proactive planning and the implementation of the proper solutions, you can deal with each event effectively.

References

Carvey, H. "Detecting and Removing Trojans and Malicious Code from Win2K." September 18, 2002. URL: http://online.securityfocus.com/infocus/1627 (October 26, 2002)

Osborne, Tia R. " Building an Incident Response Program To Suit Your Business." July 3, 2001. URL: http://rr.sans.org/incident/program.php (October 26,2002)

Borodkin, Michelle. "Computer Incident Response Team." September 15, 2001. URL: http://rr.sans.org/incident/CIRT.php (October 26, 2002)

Symantec Corporation. "Responding to Attacks." Virus Protection and Content Filtering in the Enterprise. Cupertino, CA: Symantec Corporation, July 31, 2002. Unit 5

Maley, Brent. "Network and System Planning – How to Reduce Risk on a Compromised System." September 18, 2001. URL: http://rr.sans.org/malicious/sys_planning.php (October 26, 2002)

[4] Klinder

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Klinder, Bernie. “Computer Virus and Malware Primer for Network Administrators.” October 25, 2002. URL: http://www.labmice.net/AntiVirus/articles/avprimer.htm (October 26, 2002)

netForensics. “Making Security Management Manageable.” November 26, 2001. URL: http://messageq.ebizq.net/security/netforensics_1.html (October 26, 2002)

Bakman, Alex. “The Weakest Link in Disaster Recovery.” URL: http://www.net-security.org/article.php?id=174 (October 26, 2002)

Symantec Corporation. “Securing instant messaging”, Spring 2002 Issue 14 URL: http://www.symantec.com/symadvantage/014/instant.html (October 26, 2002)

Hulme, George. “Tools provide centralized management of security applications and data.” January 7, 2002. URL: http://www.informationweek.com/story/IWK20020103S0010 (October 26, 2002)

© SANS Institute 2003, Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced