Detecting And Recovering From A Virus Incident—Part 1

John Stone

Viruses and other malicious code costs everyone countless hours of downtime and frustration. Here is one expert's advice on how to handle an attack.

When it comes to new viruses and malicious code, enterprise IT shops and antivirus software providers can only react to the latest threat, not pre-empt it. Short of dismantling IP networks, there is no way to totally protect IP endpoints from the next email or Web-based virus.

That's discouraging, but it doesn't mean enterprise IT shops are powerless. In fact, experience demonstrates that specific and effective steps can be taken—even if you lack the latest tools or infrastructure. This article will explain how to detect a virus and, if you discover that you are infected, what immediate response and stopgap measures you should take.

Next month, in Part 2, we will cover cleaning up the environment and some longer-term process improvements. For the purpose of this discussion, all malicious code will be referred to as a virus, although this is technically inaccurate in some cases. Let's start with a review of how these bits of code manage to get into the corporate IP network in the first place.

Identify The Attack

Email has been the most visible method of virus distribution, but it is not the only way that viruses can enter your IP network environment. For example, end users may bring infected floppy disks from home, or they may perform FTP or HTTP downloads from infected sites. Most recently, virus writers and intrusion experts have been cooperating to develop viral code that enters networks by exploiting known application security bugs in various applications.

Once a virus enters your network, it spreads from computer to computer in multiple ways. Some viruses search the network for systems that are configured to allow file sharing and try to access and infect their files. Other viruses email themselves to nodes on the network. Some do both, while others spread in unexpected ways, including the use of instant messaging systems or peer-to-peer applications. A single infected computer in your network can quickly infect many other systems on the IP network.

Is It Really A Virus?

If your antivirus software can detect an infection or an infection attempt, it can usually deal with the situation effectively, thus you will not have a virus incident. Virus incidents are caused when a virus is able to escape your antivirus and/or intrusion detection screen. When this occurs the virus will typically signal its presence, either as a direct result of its attempt to spread or as a side effect. Common indicators of virus infection include:

- Unexpected sounds or screen images, especially if these occur on multiple systems, can be the virus payload. While these indicators are nondestructive, this does not mean the virus itself is not destructive. You must educate and then depend upon your users to detect and report these interface indicators.
- File indicators are the most common but often the hardest to detect. They include the appearance of multiple unknown files on user workstations 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, files that contain executable code may suddenly change size, as the virus inserts itself into the code and 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 (IDS).

- System indicators are usually easy to detect as they often interfere with the ability to use the system. Examples include the unavailability of file partitions 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 effect of poor programming on the part of the virus creator—but it

John Stone is a principal security consultant for Symantec Security Services specializing in protecting network environments from the effects of malicious code. He can be reached at jstone@symantec.com.

Once you identify the virus, you must determine the scope of infection and how it spreads

can also be the result of a so-called logic bomb, a bit of malicious code put in place by the creator to execute on a specific date or based on some other trigger. Your users will always let you know about this type of indicator.

- Network indicators are usually caused by the side effects 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 own environment specifically for detecting new viruses not detected by antivirus software. For example, you might want to set up a dummy Microsoft Exchange email group list account including only dummy user accounts so you can detect email worms that use Microsoft Outlook to spread.

While many virus indicators can be easily tracked to a specific action or a specific trigger, in some cases the indicator can occur at random, unpredictable times. These indicators are the hardest to track and to determine if a virus is, in fact, causing them.

Background Research

Weeding out the non-viral indicators is the first step. Joke programs, advertisement messages, application errors, common user mistakes, system failures and network hardware failures are among the events that can trigger confusing indicators. Here are several sources that can help you identify the known viral and non-viral issues that could cause the same indicators:

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

Identify And Assess The Infection Vector

Once you determine that a virus is causing the indicator, the next step is to identify the nature of the attack. Ideally, you should take the time to fully determine which systems are affected, but some viruses can spread faster than you can assess their impact. Infections that can't be quickly addressed by updating your antivirus software require further diagnosis before a plan can be made to eradicate them.

To decide how to proceed, you have to know which virus you are dealing with and the possible repercussions to your environment. Educate yourself on how the virus spreads, its method of attack, and the possible damage it can create. You need not depend solely on your antivirus or intrusion detection vendor for virus information, although you should consider them the arbiters for conflicting information. Consider the following sources:

- Virus Protection software vendors, such as McAfee, Sophos, Symantec and Trend Micro.
- The Computer Emergency Response Team (CERT) website: www.cert.org.
- Major news websites including CNN (www.cnn.com) and MSN (www.msn.com).
- The Virus Bulletins web site: www.virusbtn.com.
- The International Computer Security Industry Association website: 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 website: www.infosyssec.net/.
- The National Institute of Standards and Technology: csrc.ncsl.nist.gov/virus/.
- Security Focus: www.securityfocus.com.

Once you have identified the virus, you must make an educated guess concerning the scope of the infection. Ask these questions to assess the infection vector and to identify the fastest ways to stop the virus from spreading:

- How does it arrive in the network?
- If it arrives via SMTP email, content filtering may stop it. If it arrives via browsing to an infected server, you can block URLs. If it arrives via peer-to-peer applications or Internet chat applications, try blocking the specific ports used by these applications at the firewall.
- Is it network-aware and does it propagates via file sharing? If so, it is more likely to have spread to other systems unless you remove administrative shares and disable file-sharing capabilities as a regular practice.
- Does it use groupware or email gateways to further propagate? If it utilizes internal email systems to spread, again, content filtering on those systems may stop it. If it installs its own SMTP server to send email instead, you may want to temporarily block port 25 at the firewall.
- Does it enter the environment through security holes? If so, you might be able to apply software patches to stop its infiltration.

You must also assess the spread of infection. Check all high-priority administrative and high-availability computers and, if any are infected, disconnect them from the network. As these systems

Immediate Response: Update Your Antivirus Software

Assuming you have antivirus software installed in your IP network, the first thing to do *whenever* you suspect your environment has become infected with a new virus is to determine whether your antivirus vendor has released an update that will detect the infection. Hopefully this is the case, and the vendor will also have a repair methodology available.

Install the updates to detect and repair the virus by following these steps:

- Obtain the detection signature for the virus from your antivirus vendor.
- Obtain a technical description of the virus from your antivirus vendor.
- Test the detection signature update provided by your vendor in your virus signatures staging lab (if available).
- Distribute the fix to your network environment; using whatever method you have in place for rapid deployment.

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

Submit A Sample File

If the latest virus signatures do not detect the infection, submit a sample to the antivirus vendor for analysis and signature creation. This is usually a straightforward process if the virus was detected and stopped but the antivirus software was unable to repair. In fact, most antivirus software itself can perform the task of obtaining the sample.

With a new virus or a new virus strain, you should locate and submit a sample. While it is true that your antivirus vendor will most likely obtain a sample eventually, it is also possible that you are among the first victims, perhaps even the only victim. In these cases, it is very important that you obtain a sample for your vendor. Call the antivirus vendor's technical support line to learn how to obtain the sample correctly□

Pull together a response team to assess options, recommend fixes and get them implemented

are more likely to have been accessed by other systems, the virus is likely to have spread further. Consider removing uninfected servers from the network to prevent their infection.

If the virus is network-aware, check to see if any network administrator accounts are compromised. This is often caused by infection of a network administrator's system. Once this occurs, a network-aware virus is more likely to have spread further. You may need to disable the affected user accounts.

Call In The Reserves

If you haven't done so already, now is the time to gather a team to deal with the threat. This team is responsible for determining options, recommending the proper solution and implementing the selected solution. Use your incident-response team and incident-response-procedures, if you have them. If not, you need to pull a team together. (Part 2 of this article, next month, will discuss how to create and operate a virus command center.)

Designate a team leader who will be responsible for driving through the process of resolving the virus infection, and consider the following resources for your team:

- Help-desk personnel often raise the initial alarm, and continue to receive calls from users complaining about the indicators. They can communicate the response processes to the users.
- 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 and server operations personnel can track down infected systems, identify high-priority protection points and communicate the response process to users. Both teams may need to patch systems as part of the response process.
- Network personnel may need to block connections at the perimeter and/or segment the network to contain the spread of the virus. They can also audit firewall and router logs to locate initial infection points.
- The messaging team may be called upon to down or to reconfigure the email servers, or to patch them as part of the response process. They can also audit email logs for indicators of initial infection points.
- A legal representative may be needed to assist in forensic investigation activities after the virus is contained.
- 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 or response affects business partners, customers, or others.
- Human Resources may become involved if the virus incident resulted from an employee or contractor violating policy.
- Upper-management involvement may be needed if response decisions are likely to negatively impact the company, its partners, customers or others.
- Representatives of affected business units and departments must be kept apprised.

To regain control of your network, you must locate and clean every infected system

■ As part of the recovery effort, you may wish to bring in external assistance (This will be discussed in more detail in Part 2).

As you begin the response process, you need to determine how to communicate the problem to all teams, how to escalate the problem properly, how to track solution progress and when to bring each team into the response process. Clear communication is invaluable in helping determine the cause of the virus, the initial infection points, the spread of the infection, and in coordinating the proper response.

Containing The Attack

It isn't always sufficient to update your antivirus definitions and scan your systems to remove the virus from your environment (see "Immediate Response: Update Your Antivirus Software," p. 45). You must locate all systems that are infected and clean each of them completely in order to regain control of your network (see "In Search of System Zero"). In many cases, this is a lot easier said than done, and it can take a while. At the same time, you should be taking steps to contain the continuing threat.

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

All containment activities should be controlled centrally after notifying the affected parties. These may include individuals in charge of messaging servers, webservers, Internet access, file and print servers and/or application servers. It is sometimes easier to determine who is affected based on departmental division or network location.

If the virus can spread through email, HTTP or FTP access, concentrate on updating the protection on your email/groupware servers, proxy servers and SMTP email gateway servers first; these are the fastest means of spreading the infection internally and externally. Updating protection may entail installing software patches, updating virus signatures, implementing content filtering, or other measures.

If the infection is spreading faster than you can distribute the fix(es), you probably will want to contain the attack by disabling services that allow incoming requests. This is especially important in the following situations:

■ When antivirus signatures are not yet available from the vendor.

■ When content filtering is not possible due to changing content.

■ When users are not properly educated concerning the virus threat and their role in protection.

Refer to the vendor's technical write-ups on the virus, if these are available, when considering containment actions. Possible actions 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.

■ Change content filtering software to block email containing certain strings of text.

■ Block Internet HTTP or FTP access.

■ Consider sending users home in departments that are severely affected by the outage, or remove

In Search Of System Zero

Containing the attack is important, but it is also crucial to avoid re-infection by finding and eliminating all sources of infection in the network. Start by establishing system zero(s), the first systems attacked; it is then easier to determine which systems or services to deactivate. Consider the following tactics to find system zero:

■ Use network traffic analysis applications to track the spread of the infection.

■ Compare time stamps on system files between systems to determine the path of infection by determining when files were created or changed.

■ 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 systems that face the Internet, including gateway and messaging servers.

■ Identify new workstations placed on the network, as they often carry 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 effects of the virus□

unaffected workstations from the network, allowing users to continue work locally.

- Consider write-protecting critical data accessible to the virus on high priority systems.
- Create dummy files on non-infected systems to prevent infection of the system.
- If the risk is extremely high, completely disconnect the network from the Internet.

You should also consider disabling services that provide 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.

Conclusion

If you can accomplish all the above, you have made a good start on recovering from the virus attack. You will also want to check with business partners, customers, contractors and temporary employees, as well as other parties who may have been infected, or are at risk of infection through their IP connections to your network. Part 2 of this article will cover the rest of the cleanup effort, plus suggestions for longer-term improvement of response processes.□

Companies Mentioned In This Article

CERT (www.cert.org)

CIAC (www.ciac.org/ciac)

Computer Virus Myths (www.vmyths.com)

ICAT Metabase (icat.nist.gov)

ICSA (www.icsalabs.com/html/communities/antivirus/index.shtml)

Information Systems Security Professionals portal website: www.infosyssec.net/

McAfee (www.mcafee.com)

Microsoft (www.microsoft.com)

National Institute of Standards and Technology (csrc.ncsl.nist.gov/virus/)

NTBugTrack (www.ntbugtrac.com)

SANS (www.sans.org)

Security Focus (www.securityfocus.com)

Sophos (www.sophos.com)

Sun (www.sun.com)

Symantec (www.sarc.com)

Trend Micro (www.antivirus.com)

Virus Bulletins (www.virusbtn.com)

Check with business partners, customers and anyone else who may be affected by the virus or by your response