Detecting And Recovering From A Virus Incident—Part 2

John Stone

After you identify and recover from an attack, the hard work really begins.

Cleaning up after a severe virus infestation can take weeks in a large enterprise IP network. Unfortunately, no matter how thorough the cleanup, it won't prevent a subsequent infection from the next new virus. But don't let this discourage you from thoroughly investigating the current virus attack, or from making policy and procedure changes so that you can respond more effectively next time.

Even if you can't afford to staff a full-blown security command center (see "The Security Command Center," p. 60), it's worth considering ways your staff might reduce response time, better coordinate information flows, direct containment activities, perform virus research, receive instructions from antivirus vendors and interface with business units and upper management. In fact, good communication is probably the key to effective cleanup, investigation and security improvement efforts.

Creating A Cleanup Procedure

A clear and concise cleanup procedure, created with input from all teams involved in the process, will help everyone do their jobs efficiently. The effort will include personnel from the help desk, messaging, Web server administration, server operations, workstation operations and other work groups (see *BCR*, March 2003, pp.42–47).

Cleanup starts by obtaining updated virus signatures, removal tools or written removal instructions from the antivirus vendor. The signatures and/or removal tools should be tested and distributed to all systems. In some cases, you may need to create your own script or manually run the antivirus vendor's removal instructions. These are typically included in the virus technical write-ups.

On infected systems that do not have antivirus software, it is usually advisable to remove the virus before installing antivirus software. It is often more cost effective to recover systems using stored system images than by attempting to repair the damage. Altered files can be restored if the previous files have been stored on backup servers.

For a good cleanup process:

- Obtain the virus signature and fix tools from your antivirus vendor.
- Test the fix in your virus signatures staging lab, if you have one; otherwise, on non-critical systems in your production environment. This includes testing any repair tools that must be run before using the updated virus signatures.
- Develop a workable method for deploying the repair-and-fix process.
- Create a plan detailing how you will repair the damage and deploy fixes, where you will start and how the process will proceed. Validate this plan with all affected teams and your antivirus vendor. Plan to first clean all infected perimeter and email servers and update their virus signatures.
- Distribute the fix to all workstations and servers in your environment.
- Isolate systems that require repair.
- Run all required fix tools on all infected systems to remove the virus or disable it.
- Scan all systems with the updated virus signatures to remove all infected files.
- Eliminate all temporary and suspicious files, including hidden directories and files.
- Remove or alter configuration information used for the functionality of the virus or that might allow the virus to reappear.
- Remove configuration information that may cause system failures.
- Search for newly mounted partitions created by the virus and eliminate them.
- Search for missing log partitions and restore.
- Search for added or altered user accounts and remove or restore.
- Restore changed or deleted files.
- Update the security patch levels on all systems to help prevent re-infection.

Help-desk personnel often can lead and document the cleanup project, in conjunction with the on-site IT personnel performing the actual cleanup duties. Managing the project to completion also will be easier if you have administrative policies and procedures in place. Use written forms to track progress and to ensure all systems

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.

are cleaned and/or patched. Conduct spot checks and have two separate teams monitoring progress to be sure that proper procedures are followed. Whenever possible, use teams and team members who are familiar with incident management, virus management and vulnerability management.

Don't try to perform in-depth forensics—bring in an expert

Investigate The Cause

There are two reasons for investigating the cause of a virus attack. One is to understand which vulnerabilities were exploited, so that you can mitigate this risk in the future. A forensic investigation will provide additional information that you can use to increase security against virus intrusions.

Another important reason to investigate is to gather evidence for possible civil or legal prosecution. Assume that prosecution will occur until decided otherwise. Such evidence usually includes any files changed or left behind by the virus.

One of the first things to determine is if the attack was targeted at your environment and, if so, whether employees or former employees were involved. If this proves to be the case, a forensic expert will probably be required.

The forensic expert will extract the needed information from the compromised system(s) without altering the original data. Preserving information is crucial to interpreting the degree to which malicious activity has occurred, and to understanding the extent of the incurred damage.

You may do more harm than good trying to perform in-depth forensics yourself. If you suspect

The Security Command Center

If financially feasible, every large company should have a security command center. Besides enabling the company to respond efficiently and effectively to virus and other attacks, the center can perform virus research and coordinate data gathering and information, deal effectively with antivirus and other security vendors and coordinate with upper management and other business units.

To function properly during a virus incident, a command center or *ad hoc* response team needs rapid access to everyone involved in the response process. Each team member should have a list of key players and their functions, so that everyone can be kept informed. Escalation procedures and contacts should be written down and distributed, as well as contact information for the legal, accounting, public relations and management representatives. Contact information and policy for notifying business partners and others is necessary because they also could be put at risk from your virus incident.

To maintain voice communications, the command center or team will need dedicated telephone lines or cellular telephone service and functional telephone equipment. An increasing number of business telephone systems are computer-based and connected to the IP network, making them vulnerable to both viruses and response processes.

To actually resolve the virus incident, the team will need fully-functional network connectivity with dedicated LAN lines, and access to central management software for the antivirus and intrusion detection systems. In addition, the following would be very useful:

- Pre-tested, two-way radio communication for the local campus in order to keep phone lines or cellular connections free for remote-site communication.
- A CD burner to create CDs for distributing software patches and updated virus definitions.
- A dedicated power supply for the command-center room or the building, with a backup power source also available.
- Pre-tested, virus-free systems with all current antivirus and content filtering software installed. These are used to create patch CDs, test repair processes and any updated virus signatures or tools provided by your vendors.
- The command center should have its own LAN segment to provide a level of protection against virus infection.
- The command center should have separate Internet access, bypassing the corporate LAN, so the center can continue to access Internet resources even if the internal network is taken off the 'Net.
- Periodically—and not in the middle of a virus response—you should test the command center's telephone, computing and network resources to be certain they are working.

Proper Use Of A Command Center

Not every virus incident will require use of the command center. If the virus is slow-spreading and can be eradicated within a day, using the command center is probably overkill. But you should activate the command center if a virus is spreading quickly through email or through the IP network, if it reduces productivity for a significant number of users or if it has spread or could spread from your IP network to that of your customers, business partners or others.

When you first enter the command center, contact the appropriate upper-management representative to alert them to the incident. Then contact the key response-team players to inform them. Ask them to assist as necessary, and be sure to keep them informed if they are not actively participating. Provide your location information and obtain theirs to ensure continued communication availability□

any involvement of internal staff, or the loss of data confidentiality, contact a forensic expert.

Until the forensics expert arrives, protect the evidence by taking the following steps:

- Choose one system to set aside for forensic purposes, preferably system zero, the first one infected (if it can be identified), as it may contain evidence not present on systems infected later.
- Do not make changes to the selected system unless otherwise directed by the forensics expert, or to protect data on the system or to stop the virus from spreading.
- Ensure that normal system operation does not overwrite data—if necessary, disconnect the system from the network. But turn the system off only to prevent infection of important data, since downing the system can corrupt evidence.
- If the infected machine is a critical system that you cannot afford to disable, then back up key system files including configuration and registry files and logs before the information is lost. This information may not stand up as legal evidence but can assist in the investigation of the originating cause.

Improve Policies, Technologies And Procedures

Do not gamble with the security of your IP network. To mount the most effective protection possible, find and address the weaknesses in your policy foundation and security point solutions.

A good security policy foundation includes high-level goals, standards to use in meeting those goals and processes used in meeting the standards. In determining where changes may be needed in your organization, consider the following:

- Update written policies to address new threats. Do you need proactive, centralized, intrusion-notification solutions? What about content filtering of email, Internet and network traffic, or blocking of high-risk Internet resources?
- Include enforcement as part of the security policy. Systems that violate policy can be disabled automatically and the people who thwart policy can be sanctioned through HR policies.
- Create incident response procedures and put together a virus response team.
- Clarify or adjust the reporting structure and communications processes within the technology departments and among the teams, to simplify infection response processes.
- Educate users and make sure they know whom to contact when they suspect a virus infection.
- Educate upper management on the importance of proactive virus protection.
- Require backup servers for all critical files.

Once policies have been updated, the technology infrastructure may need some changes to implement the policies, including:

- Install antivirus solutions to filter email, Internet and network traffic and local file access.
- Implement centrally managed antivirus software to control configurations and keep virus signatures current.
- Install both host-based and network-based intrusion detection technology. Host-based intrusion detection can detect viruses that the antivirus software may miss. Network-based, intrusion-detection technology helps determine the spread of the infection. Newer network intrusion prevention technology can even help stop the spread of the infection (see *BCR*, March 2003, pp. 36–41).
- Install security management software to monitor policy adherence and system patching.
- Simplify the network topology so it can be easily segmented during a virus infestation.
- Install email content filtering technology to block email based on strings of text in the subject line or the body of the message.
- Implement an internal Instant Messaging (IM) solution so that users do not have to use an externally-controlled solution.
- Implement desktop firewall software to block the spread of a virus through specific ports. Desktop firewalls are especially important with the advent of VPN and wireless solutions.

Updates to the policy and technology will probably also dictate some changes to your administrative processes. For example, you may need a full-time antivirus administrator, or you may want to consider outsourcing this function.

Optionally, you may want to outsource the management of antivirus protection for a particular site, subnet(s), server(s) or function(s). This is especially effective for perimeter subnets or perimeter devices, such as SMTP servers.

Routine backup procedures should be in place and compliance monitored. This will ensure a minimum loss of data in the event of an aggressive attack. Other basic improvements include:

- Prevent users from disabling antivirus software.
- Limit the allowable file extensions for email attachments.
- Implement a process in order to keep system patches up to date.
- Institute technology or processes to verify that antivirus software is running and up to date.
- Lock down workstations to limit regular users' ability to modify their systems.
- Disable the Windows Scripting Host, as it is not often needed by users and provides a known propagation method. You may also want to re-move scripting in Outlook and Internet Explorer.
- Disable the ability to access external IM systems, news groups, email servers or other externally-controlled communication platforms.

Conclusion

Viruses and malicious code are the frustrating, but unavoidable offspring of today's open and flexible IP networks. Because each virus event differs from the last, there is no magic bullet or complete defense. But with proactive planning, vigilant enforcement and appropriate technological solutions, you can deal effectively with each event□

In the wake of an attack, find and fix weaknesses in your policies and technology