What To Do Before, During, And After A Malware Attack

Don't let a malware attack ruin your business. A little planning and the right responses can make it a minor annoyance instead of a major catastrophe.

by Ross M. Greenberg

1. Preparing For Attacks

- Always use licensed software, and keep all software on every system up to date with the latest critical patches.
- Scan all systems regularly to ensure they are virus-, Trojan-, and spyware-free. Make sure your security software protects all network entry and exit points and that it's updated with the most recent signature files.
- Back up all systems on a regular schedule (weekly is good; daily is better).
- Subscribe to security vendors' e-bulletins so you'll be aware of current vulnerabilities, patches, and exploits.
- Set up a response team that includes a member of management as well as technically competent people who are knowledgeable on malware and security matters. This team must be available 24x7.
- Set up a telephone list of people to contact if a problem occurs. Expect that a problem will occur at the worst possible time, such as at midnight on New Year's Eve.
- Make sure that all appropriate personnel have hard copy for all pertinent contacts. Presume that the malware attack will take out all access to your electronic data.
- Have temporary backup/replacement systems (these should be clones of your most sophisticated systems, with large hard disks and sufficient memory) in case you need them; be able to restore your systems from those backups, if required. You need to have enough clean systems to be able to use them to clean up the dirty systems one at a time. Copy the whole hard disk, and make sure you're working with full system disk images -- boot images too!
- Restoring systems will involve restoring data from firewalls. Know pertinent port numbers and so forth. This, too, should be available in hard copy.
- Most attacks are introduced unknowingly by insiders. Educate, educate, educate your users.

2. Recognizing An Attack

Pay attention to the most common warning signals (all of which will be unexpected and unexplainable):

- System slowdown
- High network activity
- Sudden file/disk activity
- Gateway system slowdown
- Remote sites suddenly not available (though it's possible that those sites and not your system are under attack)

3. Responding To An Attack

- Disconnect compromised systems from networks. However, do so carefully: Some malware programs do regular checks to determine that "member systems" -- infected systems on a network -- are still connected. If the malware finds that any of the previously infected systems are not on the network, the payload may activate.
- Clean the infected systems using the anti-malware software you already have in place. Make certain that the signature definition files are up to date -- expect that the really dangerous malware executable signature was in last night's signature file.
- Determine what the actual target of the attack was and check its integrity. If it's clean, make a backup. The malware's malicious payload may not have been activated yet. Clean up your systems before it does.
- Determine the entry point of the malware problem. This will help you secure the network, servers, and systems from being the entry-point next time.
- Assume that the malware did more than attack a few copies of Solitaire and that your business systems have been compromised. Further, assume that you may well have missed an infected system in the cleanup effort -- think about the possibility of stealth infections. Run scans on systems booted clean from write-protected floppies, from CDs, or from safe partitions to be sure the system being scanned is infection-free.
- Systems get infected with malware all the time. It happens. Don't be ashamed and try to handle the problem by yourself. Your response team should include some real experts; use them. It's what they get paid for.
- For experts only: If you know what you're doing, allowing a virus, worm, or other malware to spread on your system and watching it as it does so can be quite enlightening. If you're not sure you can contain it, though, don't risk it!

4. Restoring Services And Systems

- Change all passwords on all systems and servers.
- Make sure to restore only from clean backups, made from systems that have been checked for malware.
- If your system(s) came under active attack, it may again. Examine all firewall logs to try to determine the source IP of the attack.
- Scrupulously monitor all network activity to be sure the malware isn't still lurking around and new back doors haven't been created.

5. Replaying The Response

- Get the malware team together to discover what can be learned from the incident.
- Determine how effective the team's actions were and whether these actions can be made more effective. The team's management representative should be able to implement suggested changes as required.
- Tell the story of what happened to upper management to prepare them for the next time. If nothing happened aside from the attack itself, great! Your planning worked perfectly.