

# Malware Response Plan

In protecting networks against worms, Trojans, and other viruses, every organization must follow an established response plan. This chart provides the basic steps to follow when confronted with a threatening incident. Yet, as every infection situation is different, you can use this chart as a template to

customize plans when dealing with specific viruses, such as Bagle, by adding additional remedial steps and actions. Print out this chart, as well as customized virus response charts, and post them in prominent and convenient locations for your IT staff's use.

## Before an incident occurs: Establish procedures

Establish written procedures with checklists, and separate the process into two separate categories:

1. Locating, removing, and verifying removal of the infection
2. Restoring data and services (This can be assigned to the same individual(s) but you need to keep the processes separate.)

Designate and train an incident response team: This must include more than one person, even if that requires an outsourcing agreement, because you must always have someone available.

- Select team members: Designate precise chain of command, responsibilities, and authority.

- Secure communications: Keep hard copies of cell phone, pager, and other contact information, including encrypted e-mail addresses where on-duty personnel can always locate them.
- Obtain forensic software and train team members to use it.
- Have standby hardware, blank media, and a portable printer: You will need to record everything, or you'll never know what damage may have occurred.
- Maintain current and accurate port list, network map, and baseline activity statistics, as well as full documentation: **Keep a separate copy of antivirus software as some malware deletes antivirus software.**

## Detecting malware: Common infection indications

- File integrity/change-monitoring software reports
- IDS or antivirus software triggers a warning
- Web server crashes
- Workstations freeze or slow dramatically
- Internet access slows dramatically
- A surge in the number of bounced e-mails
- Significant deviation from baseline activity

## Containment procedures: First steps to take

- Isolate infected system(s): Disconnect from Internet, wireless net or wired network, and disconnect the modem if applicable.
- Notify the designated on-duty incident response leader: You've got an expert with authority to make decisions; be certain he or she knows what's happening.
- Consider powering down the machines: Some infections will cause additional damage if disconnected from the network; e.g., if they ping another host, the pings will fail and may overwrite hard drive data. Develop written guidelines on this.
- Secure backups: Don't install your only backup unless you are positive the system is clean—keep at least one backup safe. If you want to duplicate a backup, do so only on a dedicated, isolated system.
- Secure system logs: This is essential so you can later determine if there was any damage.
- Record incident details: Write down (on paper) time, machine ID, symptoms, and any/all actions taken. Don't assume you will remember the details; you never know who will be on duty when an incident occurs.
- In rare instances delay containment to monitor activity: This is potentially very dangerous and only a designated incident response team leader should make that decision. Develop written guidelines on this.

## Remove infection: Basics (Viruses typically require specific removal steps as well)

- Disable and delete malicious code: Where possible, use commercial tools for this. Even antivirus vendors may recommend that you use a special free tool because their normal removal procedures may not be completely effective on blended threats.
- Install and run antivirus software with the latest signature file: Do this after using any removal tool and make certain the latest data cover the threat you just removed.

## Determine damages: Investigate extent

- Locate the source of infection: Find how it entered the system—this will aid in locating damage as well as preventing future incidents. Insider attacks are common and the most dangerous.
- Determine the payload: Leave this to the pros, such as an antivirus vendor's Web site. Don't attempt in-house unless you have a dedicated security staff with lots of experience; it's too easy to miss something. Even the experts sometimes don't discover a backdoor until hours after the initial reports.
- Check to see if the payload was actually activated: Do this by verifying the integrity of code or data that would be attacked by the payload.

## Restore services

- First disable compromised or potentially compromised accounts.
- Change all passwords.
- Increase network monitoring level: Not only was something obviously wrong with your security, you are also more likely to be attacked again. There may even be a new backdoor you missed.
- Restore system and data from trusted backup: This is the very last step other than testing to verify that the system has been restored to normal.

## Debrief incident response team

- Measure response effectiveness: Perhaps you did too much, too quickly, but the chances are that you need to improve response time and add new steps.
- Prepare and add new information to the incident response plan: This should be provided for in the basic IR plan, and someone on the team should have the authority to make specific changes.
- Report results to management: Prepare a detailed report for upper management, including an honest evaluation of the team's response, damage estimates, and any major recommendations for procedural changes.

## What not to do

- Don't ignore warning signs: It may be a false alarm, but if something appears to be going wrong it's likely that you are either under attack or you have some internal system problem that requires attention.
- Don't risk compromising backups before the system is completely purged of infection. That should be pretty self-evident.
- Don't wait till the first incident before preparing your defense: You will be attacked, or will think you have been attacked at some time. It's too late to prepare or plan then.
- Don't delay **critical** patches: These sometimes cause problems but you know someone is likely to use them to attack your system, and it's difficult to explain to your boss why you ignored a known threat.
- Don't skip regular antivirus signature updates: Although essential, this isn't a sufficient defense. Weekly updates don't help much when malware spreads so quickly.