How do I remove malware and recover from a system compromise?

How do I remove malware and recover from a system compromise?

On this page:

Answer

Important!
If you suspect a compromise on your computer and handle any Personally Identifiable Information (PII), Protected Health Information (PHI), or other data classified as High Risk, do not format your computer or attempt to fix it. Stop immediately and contact the Data Incident Response Team at infoprotect@mit.edu.

Disconnect and Report

1. If possible, to preserve logs and data, DO NOT shut down/power off the computer. (See further information below on preserving logs and data.)
2. DO disconnect the machine from the network.
   This will prevent an attacker from doing further damage to your system, and from using your system to attack others. To disconnect your machine, simply unplug the ethernet cable, or if the computer uses a wireless connection, turn off the wireless access in your system settings. If you are not sure how to disconnect from the network, contact the Help Desk at 3-1101.
3. Send an email report to security@mit.edu. Try to use another device or one of the public Athena workstations for emailing. Include the machine name, operating system type and version, contact person, and any other information relating to the suspected event. If unable to email, call the Help Desk at 3-1101 and provide them with the incident information.

You will receive a response from IS&T with further inquiries and instructions regarding your case.

If the compromise was detected by IS&T, the Security team will quarantine the computer from the MIT network to contain the compromise. We will also attempt to determine a good contact for the computer and send a notification email.

Preserve Logs and Data

1. It is important to preserve system logs and other data that might be useful in tracking the source and nature of the intrusion. **Very important:** DO NOT turn the machine off or reboot unless instructed to do so by IS&T. It is possible that changes may be made to your computer during or after reboot, which will make it more difficult for IS&T to determine the cause of your problem. Leave your computer powered on and disconnected from the network unless otherwise instructed.
2. To preserve system logs and other data, DO NOT use the machine after it has been disconnected from the network.

Steps to Recover from Malware

The only reliable way to remove the malware is to reformat and re-install your operating system. Reformatting a machine is required because it is not possible to detect and eradicate all possible malicious code on your machine. Many types of malware will not be detected by antivirus programs. We understand how frustrating and time-consuming this is, and we are sorry for the necessity. This is, unfortunately, the only way you can be sure that the recovery is complete.

Warning
If you are not comfortable with backing up, reformatting, and reinstalling the operating system on your computer, it is strongly recommended to contact the IS&T Help Desk.

1. Backup your files if you haven't already.
2. Format the hard drive of your device.
3. Install a vendor supported operating system, and be sure that it is set to automatically install updates. A vendor supported operating system is still receiving patches from the vendor. Windows XP, for example, is no longer supported.
4. Install anti-malware and anti-virus tools. IS&T provides Crowdstrike and Sophos to the MIT community.
5. Install a backup solution. IS&T provides Code42/CrashPlan to the MIT community.
6. Scan your backed up data for viruses before restoring to the re-imaged computer.
7. For more information about how to properly secure information at MIT, please see https://infoprotect-beta.mit.edu/.
8. If your computer was quarantined by IS&T Security, please send them an email letting them know you've completed the steps above so the quarantine may be lifted.
9. It is also recommended to change the password of any other accounts on your computer as well as your Kerberos password.
   See: Changing your Kerberos password.
10. You may need to reinstall your MIT personal certificate.

What Not to Do if Your System is Attacked

If you believe you have been the victim of an attack, there are a number of things you should not do:

- Do not launch a return attack on the suspected source system. Incoming attacks often use forged source addresses, so that any repercussions fall to an innocent third party. Denial-of-Service attacks cause damage and inconvenience to innocent parties that share network or system resources with the actual party being attacked.
  Such attacks are a violation of the MITNet Rules of Use, and it is important that you maintain "innocent victim" status.

- Do not engage in a verbal/textual "flame war" with the suspected attacker. The actual identity of the attacker is often purposefully obscured, and your response may inadvertently target an innocent third party.
  Due to the possibility of legal ramifications, attacks on MITnet hosts are a matter to be dealt with officially by experienced IS&T staff only.