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:

- Disconnect and Report
- Preserve Logs and Data
- Steps to Remove the Malware
- About Reformattting a Machine
- When it's Safe to Begin Using the System
- What Not to Do if Your System is Attacked

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, 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 you have sensitive data – financial account information, any identifying information (SSNs, ID numbers), sensitive medical information, or MIT business data – on the system, include that in your report. 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.

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 Remove the Malware

There are various options for removing malware from a computer. Unless you are a computer professional, it is not recommended to remove the malware yourself.

1. Contact the Help Desk immediately, and they will likely ask you to bring in your computer. Technicians will scan the machine with tools to detect malware. If possible, they will back up the data on the machine and preserve it, then reformat and reinstall the operating system. Finally, they will restore your data.
2. If the fundamental underpinnings of the operating system (the OS binaries) are corrupted, the only solution is to reformat and reinstall your operating system and possibly lose all your data. For this reason, is important to always have a backup of your system's files.
3. It is almost impossible to completely remove malware from a computer, but if you attempt to do so, make sure you use the latest and most up to date malware removal programs.

**About Reformatting a Machine**

Reformatting a machine is required when the nature of the infection or intrusion is such that it's not possible to detect and eradicate all possible malicious code on your machine. At this point you should not "trust" your computer for anything, including its ability to run antivirus programs that declare the computer to be "clean" or to protect any important data.

The only way to ensure that a trustable operating system is on your computer is to reformat and reinstall the operating system, as directed. We understand how frustrating and time-consuming this is, and we are sorry for the necessity. Many people at MIT have been victimized by a compromise and have had to go though this process. This is, unfortunately, the only way you can be sure that the recovery is complete. Once done, adding all critical patches before connecting the computer to the network, as well as running antivirus software, and ensuring the desktop firewall is turned on, should enable you to go back to using the computer normally.

**Warning**

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

**When it's Safe to Begin Using the System**

If the computer has been reformatted and malware is no longer detected, your system is considered secure. Send a follow up email to security@mit.edu to verify that it is safe to reconnect your machine to the network.

Once you have the computer up and running, with the operating system and data reinstalled, take these steps:

1. Change the administrator password of your computer.
2. 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.
3. 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.