Antimalware Protection, Malware Removal

Antimalware Protection, Malware Removal

Malware can disrupt, damage, or even destroy a computer. IT teams are often responsible for evaluating and repairing computers that are not running well. If a computer is performing poorly or acting strangely, it might be infected with malware. IT professionals need to know how to isolate, remove, and repair infected devices. This reading covers the steps to take to detect and remove malware.

Gather and verify

If you suspect that the computer is infected, you should gather information from the user. It is helpful to note when the symptoms started and if the user has downloaded any unusual files. If the computer has one or more of the following symptoms it may be infected with malware:

- Running slower than normal
- Restarts on its own multiple times
- Uses all or a higher than normal amount of memory

After you've gathered information, verify that the issues are still occurring by monitoring the computer for a period of time. One way to monitor and verify is to review the activity on the computer's resource manager where you can see open processes running on a system.

When looking at the resource manager, you might see a program with a name you do not recognize, a program that is using a lot of memory, or both. If you see a suspicious program, you should investigate this application by asking the user if it is familiar to them.

Quarantine malware

Some malware communicates with bad actors or sends out sensitive information. Other malware is designed to take part in a distributed botnet. A botnet is a number of Internet-connected devices, each of which runs one or more bots. Because of malware's potential ability to communicate with other bad actors, you should quarantine the infected device.

To quarantine, or separate, the infected device from the rest of the network, you should disconnect from the internet by turning off WiFi and unplugging the ethernet cable. Once the computer is disconnected, the malware can no longer spread to other computers on the network.

You should also disable any automatic system backup. Some malware can reinfect a computer by using automatic backup, because you can restore the system with files infected by the malware.

Remove malware

Once you have confirmed and isolated the malware on a device, you should attempt to remove the malware from the device. First, run an offline malware scan. This scan helps find and remove the malware while the computer is still disconnected from the local network and internet.

All anti-virus/anti-malware programs rely on threat definition files to identify a virus or malware. These files are often updated automatically, but in the case of an infected computer they may be incomplete or unable to update. In this case, you may need to briefly connect to the internet to confirm that your malware program is fully updated.

The scan should successfully identify, quarantine, and remove the malware on the computer. Once the process is complete, monitor the computer again to confirm that there are no further issues.

To help ensure that a malware infection doesn't happen again threat definitions should be set to update automatically, and to automatically scan for and quarantine suspected malware.

After the malware has been removed from the computer, you should turn back on the automatic backup tool and manually create a safe restore point. If the computer needs attention in the future, this new restore point is confirmed safe and clean.

Malware education

One of the most important things an IT professional can do to protect a company and its employees is to educate users about malware. The goal of education is to stop malware from ever gaining access to company systems. Here are a few ways users and IT professionals can protect their computer and the company from malware:

- Keep the computer and software updated
- Use a non-administrator account whenever possible
- Think twice before clicking links or downloading anything
- Be careful about opening email attachments or images
- Don't trust pop-up windows that ask to download software
- Limit your file-sharing
- Use antivirus software

When all employees are on the lookout for suspicious files, it's much easier to prevent malware and viruses from taking hold.

As malware gets more sophisticated, the chance of malware eventually infecting the computers you manage becomes more likely. These steps will help you when and if that time comes.

Key takeaways

Malware can be devastating for a company's computer network. As an IT support professional, you should be familiar with how to detect, isolate, and remove malware from the computers you manage.

- An infected device should be isolated from the local network and internet as soon as possible.
- Antivirus and Anti-Malware software is a key tool for detecting and removing malware.
- Keeping threat protection software updated makes malware removal faster and easier.
- Education is the first and best line of defense against malware.

Mark as completed