Common technical issues with SMB

(issues unrelated to malware removal)

Issue: User is unable to update software.

Cause: This is usually an update error resulting from the software not having permissions to perform an upgrade installation.

Resolution: In order for the software to be updated, the user must have administrator rights. Logging in as an admin in this case should allow the software to update. Another option would be to deploy the software via a deployment tool to update the currently installed software. To do this, the user must deploy the same installer that was used to originally install the program. For instance, if the user installed SMB using an .exe, and then tried to deploy the .msi, there may be issues later on.

Issue: User is unable to download definition updates.

Cause: Where software updates failing may be a result of permissions this is often a result of the CDN being blocked by a firewall.

Resolution: The first thing would want to do here is run the Malwarebytes traceroute tool. This is going to tell us what IP address or addresses SMB is trying connect to when it looks for a definition update. Once we have retrieved this information, we then will instruct the user to allow that IP address through any firewalls they may have. Just as a note: This is simplest resolution for this issue but may not be the norm. This issue often requires investigation.

Issue: User wants to deploy and install SMB silently.

Cause: Often we see that customers don't want to go to every machine and manually install the program.

Resolution: Well, the easiest way to resolve this would be to make sure the customer has the right product. In this circumstance MEE would resolve this issue quickly. However, some customers are unwilling to upgrade to MEE. So to proceed we to offer the Corporate documentation to the customer which includes a sample script for installation, registration, and silent install. Note: The support team does not support custom scripting.

Issue: User is unable to enable Malicious Website Blocking. (Mostly Vista OS and higher)

Cause: Malicious Website Blocking is dependent on 2 services, filter manager and base filtering engine. Sometimes infections may attack these services.

Resolution: To start off we want to have the customer run an MBAMcheck. This tool we list all of SMB's dependencies, specifically filter manager and base filtering engine. We often see that BFE (base filtering engine) is either disabled or missing. To fix this there are several tools we can run to restore or fix BFE. The tool choice is at the technicians discretion.

Issue: User wants to uninstall SMB completely.

Cause: The user may no longer wish to use the computer or may simply want to transfer SMB to another machine.

Resolution: When uninstalling SMB from a computer normally, certain registry keys may be left behind. To ensure that nothing is left in the machine we will use MBAMclean. This tool will remove all SMB entries on the system and then prompt for a reboot.

Issue: User is getting huge number of detections when SMB is installed on a server.

Cause: Even though we know server operating systems are not supported, we often see SMB installed on servers. We do not support server operating systems because SMB detects its own database as threats in that environment.

Resolution: Here we have a few issues. First, is that we don't support servers in this fashion, and often tickets end at this point. Second, is that there isn't a solution and only a poor workaround. The workaround would be to disable the protection module, something many customers are unwilling to do. These tickets need to be investigated thoroughly to ensure that it is actually a false positive. However, this is a complicated process as a majority of our tools do not function on servers. We generally look for signs of an infection. If we detect anything in our investigation, we let the user know and that it will be up to them on how to proceed.

Common technical issues with SMB

(issues unrelated to malware removal)

Issue: SMB causes the terminal server to run poorly.

Cause: This is another circumstance of we don't support this but customers do it anyway. The cause of this issue is that for every instance of SMB, the resource usage spikes exponentially.

Resolution: Basically, like any issue of SMB installed on a server, it is not supported. Often we will try to assist even though it is not supported. The only thing that can be done here is to limit the number of users accessing the terminal server, which will, in turn, reduce the instances of SMB and, subsequently, reduce the resource usage.