Malware uses certificates to disable the installation of anti-malware solutions on your computer

A new malware program is preventing users from installing antivirus products by taking advantage of the digital signature check performed by the Windows **User Account Control** (UAC) for executable files.

User Account Control **prompts users for confirmation** whenever a program wants to make a system change that requires administrator-level privileges. Depending on whether an executed file is digitally signed by a trusted publisher, the UAC displays confirmation prompts indicating different levels of risk. However, if the file is signed with a certificate that was blacklisted, UAC will simply block the file from running and a red warning will be displayed.

Based on the alteration of the User Account Control in Windows, this malware prevents users from installing certain security products, by copying digital certificates that are used to sign antivirus programs to the **Untrusted Certificates** in Windows. It also keeps adding them back as untrusted if their status changes.

HOW TO REMOVE THIS MALWARE

1. Press the **Windows key + R** and type **certmgr.msc**
2. Expand the **Untrusted Certificates** tree, then open the subfolder **Certificates.**
3. Here, most of the AV certificates will be present, including Bitdefender, which is why the software is being blocked.
4. Remove all the certificates from this folder.
5. Open **Bitdefender Central**, go to **My Devices** and **Install Bitdefender.**
6. Open the main Bitdefender interface and **update** the product.
7. Wait for the update process to complete. **Don’t restart your computer**. Run a Full System Scan to remove the malware.
8. Restart your computer.

NOTE: If the issue persists, perform the above steps (1-4) **to delete** the certificates from the Untrusted Certificates tree and then follow the steps in this article to contact our Support.