Basic Malware Response Procedures

patricia falcon - 2016-04-04 - Comments (0) - Antivirus and Malware

These instructions are intended for technical staff and describe steps to take if a machine has been infected with Malware. They are generic, and mostly geared towards legacy, non-redirecting machines in the Unmanaged & Managed OUs.

If you are an individual in the Brown community and suspect you have malware on your computer, please contact your departmental computing staff or the IT Service Center immediately after completing step 1 (disconnecting from the wired and wireless network).

1. Isolate machine from network.
2. If machine holds user data, back it up to clean, dedicated removable media.
   a. While backing up, work with user to list the software applications that will need to be reinstalled.
   b. If the malware was Ransomware and has encrypted files, make sure to save any 'calling cards' left with instructions for decryption. They are typically text files. The contents of the 'calling card' should be put into the ticket. Shared drives and the user's home folder should be checked from a known-clean machine for any encrypted files.
3. Once backup is verified, use DBAN to 'zero' the hard drive.
   a. While drive is wiping, user should change their passwords in MyAccount, along with any other passwords they have used on the machine. Other users who have authenticated on the machine recently should also reset their passwords.
4. Redeploy the OS to the machine, clearing AD objects and rebinding as-needed.
5. Verify OS Updates and System Center Endpoint Protection are installed and updated.
6. Reinstall any applications the user will need.
7. Restore user data.
8. Verify customer is satisfied.