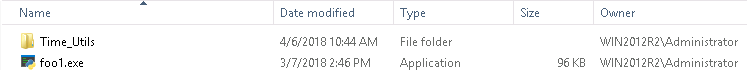
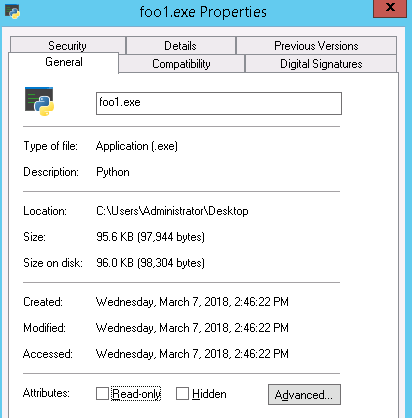
**1.3.1 – Alex Canales**

* Detect:
  + *When and by which user did a suspicious file get to your desktop?*

March , 2018

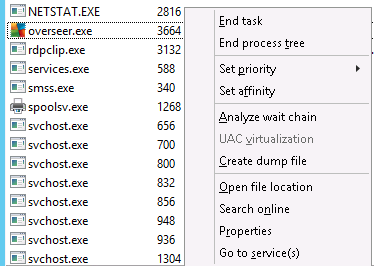
WIN2012R2/Administrator

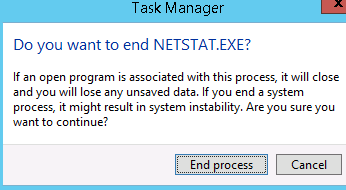




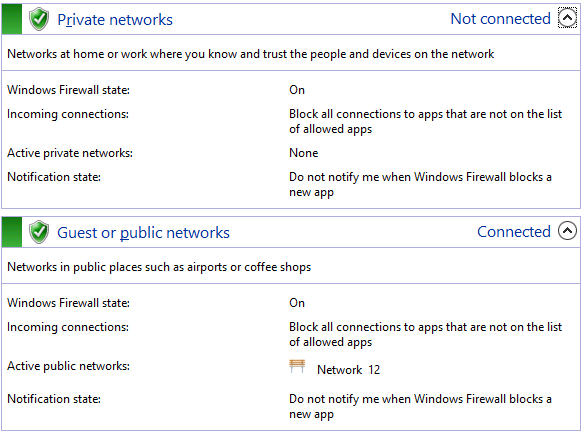
* + *Could there be other potentially malicious data on your computer? How can you find it?*

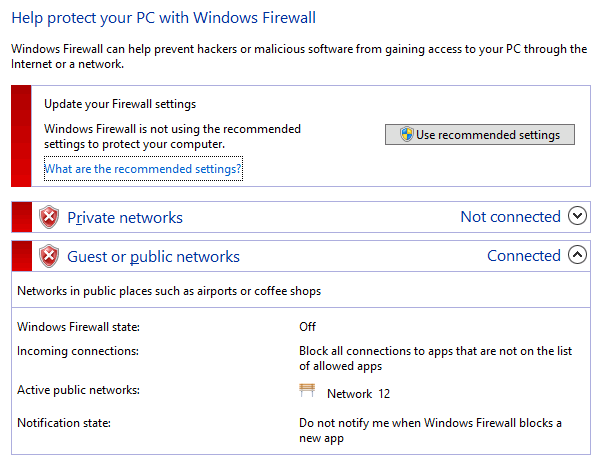
There could be by turning on hidden files. Also, the security has been breached in AVG Business and Windows Firewall and both are turned off. Searching based off date and administrator. Processes that are shared by the same Administrator and hidden are NETSTAT.exe which is a process that needs to be killed and a hidden file netstat.log.

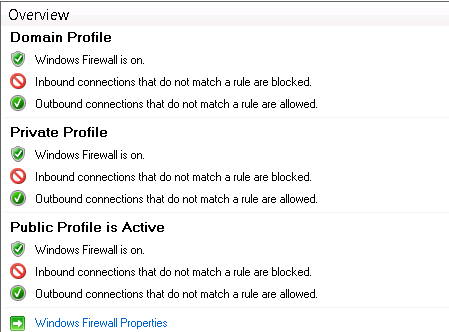


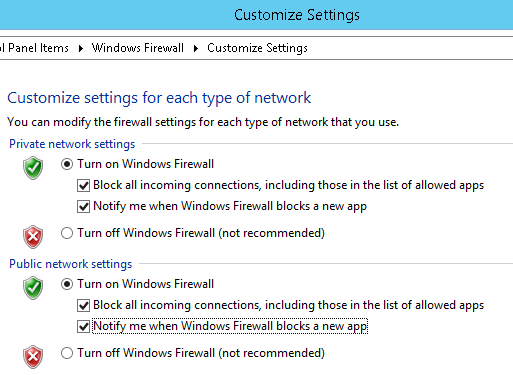


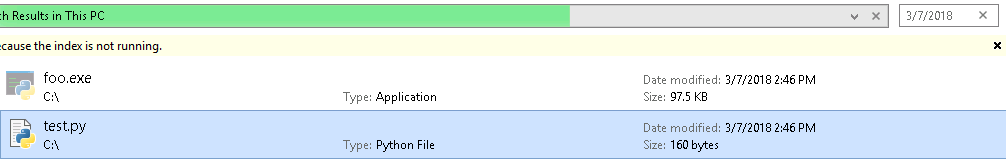
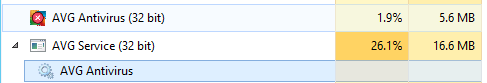
The same photos are for ending the foo.exe that permanently gets rid of NETSTAT.exe









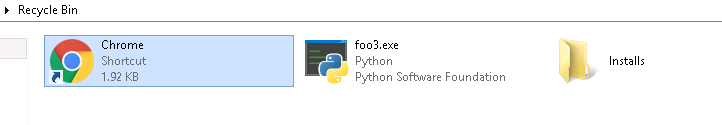


* + *What applications and/or services could have been used to get these files there?*

Chrome downloads, FTP. Windows Sharing/Downloads

* + *Are there any files missing from the computer?*

Chrome is supposedly deleted from my desktop and in my recycle bin along with foo3.exe and my installs folder



* Respond:
  + *What actions should you take to resolve the security threats?*

Redownload Chrome, foo3, and Installs folder

* Recover:
  + *How do you recover any missing data?*

Recover from recycling bin the files that were deleted

Recover deleted files in recycle bin

* Identify
  + The asset is your computer and its data.

The asset is the foo3.py file and the test.py file because they both have the same administrator and the same date modified.

* Protect:
  + *What are the security measures you should take to secure your computer and ensure this does not happen again?*

The firewall was breached and needs to be reset to protect information from the computer. Along with that check marks should be in boxes to block all incoming connections that are not included in allowed apps. Check marks should also be in both the private and public network settings.