Security Incident Response Report

|  |  |
| --- | --- |
| 1. Contact Information for This Incident | |
| Name(s) | Thomas Hughes |
| Date of Report | 9/19/2021 |
| 1. Detection | |
| Describe what was detected and the security threat, vulnerability, or breach identified.  An unknown file, foo1.exe, was added to the desktop as well as other suspicious files were found including foo3.exe and foo.exe was running in the task manager. There were also files important to the user in the recycling bin including google chrome. The firewall was disabled, and FTP was enabled allowing potentially malicious data and files to make its way to the computer. | |
| 1. Response | |
| Describe the actions you took to contain and eradicate the security threat, vulnerability, or breach.  The suspicious files were deleted and the foo.exe process was ended which also killed another suspicious process called NETSTAT.exe. I re-enabled the firewall on all three profiles and disabled FTP within the inbound rules. | |
| 1. Recovery | |
| Describe the actions you took to recover any affected data.  Check the recycle bin and confirm those items were on the computer previously and were important to the user. If needed, the files are moved from the recycle bin or the application redownloaded. | |
| 1. Identify | |
| Describe any assets you identified that need to be protected.  PLTW identifies the assets the computer and its data   * Key data could include files with important information and files important to the user in general | |
| 1. Protect | |
| Describe the actions you took to protect your assets from future threats.  Make sure the firewall is enabled on all profiles and disable all FTP traffic within the inbound rules section. Also making sure not to click on any suspicious links and verify the download of any file | |
| 1. Lessons Learned | |
| Describe two lessons your team learned while solving this problem.   * It’s important not to download / click links without knowing what they do and not running the files download without verifying them. * You should always check your network settings, including firewall, and inbound traffic before venturing out to the web and potentially encountering something malicious | |
| 1. Other Information | |
| Provide any additional information you think is important. | |