Security Incident Response Report

|  |  |
| --- | --- |
| 1. Contact Information for This Incident | |
| Name(s) | Alex Canales |
| Date of Report | 8/31/2021 |
| 1. Detection | |
| Describe what was detected and the security threat, vulnerability, or breach identified.  A random file was put on the computer that runs under the owner “WIN2012R2/Administrator” on the day 3/7/2018. My full protection has been expired in AVG Buisness and basic protection has been turned off. Files were found trashed in the recycling bin. All firewall protection was turned off and allowed all downloads to come through on FTP and from chrome. Netstat is also a hidden file and process that is connected to the Administrator and netstat.log is a hidden file added. In Task manager there is an Antivirus Software that iss using 25% of the RAM which is also a red flag that a process that is malicious was running on the computer. | |
| 1. Response | |
| Describe the actions you took to contain and eradicate the security threat, vulnerability, or breach.  Recover missing files from the recycling bin. Delete and end the tasks that were suspicious and downloaded from the user. Fix firewall protection and change settings to make it secure and only certain things to be put on the computer to confirm suspicious file are not to be put on. Ending the foo.exe task removes the NETSTAT.exe confirming that the foo task running was running the malicious NETSTAT and they were connected. | |
| 1. Recovery | |
| Describe the actions you took to recover any affected data.  Recover the missing files from the recycling bin. Change firewall settings to protect the settings that were turned off that would compromise my data in the future. Delete and end tasks that are malicious in task manager and could compromise the future processes and the computer | |
| 1. Identify | |
| Describe any assets you identified that need to be protected.  It was identified that the Owner of the files that were deleted were by Administrator WIN2012R2 that is not protected or tursted in the computer. These files were the desktop files “test.py” and “foo3.py” were added ny the administrator. Both were modified and added on the same day which is a red flag to remove these malicious files. A running task in Task manager “NETSTAT.exe” is running under foo.exe and once foo.exe is removed the NETSTAT is ended. | |
| 1. Protect | |
| Describe the actions you took to protect your assets from future threats.  Reset the firewall to protect assets from entering the computer again. 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. | |
| 1. Lessons Learned | |
| Describe two lessons your team learned while solving this problem.  1)I learned that it is really easy to hide items that look like they are supposed to be on the computer and seem like they are legit and supposed ot be on the computer when in actuality they could be malicious and not good for you or the computer.  2) Firewall is important because it really does protect the computer from malicious things to be added to the computer from downloads. | |
| 1. Other Information | |
| Provide any additional information you think is important.  I am the best cybersecuritier of all time. | |