Task 2 – Threats and vulnerabilities

* Go to the symantec website link below
  + <http://www.symantec.com/security_response/>
* Go to the threats tab and identify 5 threats and find out how they operate/ how they work.

**1) Trojan Danabot.B-**

It is a Trojan horse that steals information from the compromised computer.

**2) Ransom.Hermeslgen3 -**

It is a heuristic detection used to detect threats associated with the ransom hermes family of threats.

**3) Trojan.Betabot.B -**

It is a Trojan horse that steals information from the compromised computer.

**4) SONAR.SuspScript!g20 -**

It is a heuristic detection for suspicious script launches.

**5) Packed.Generic.534 -**

It is a heuristic detection for files that may have been obtained or encrypted in order to conceal them from antivirus software.

* Select the vulnerabilities tab and identify 5 vulnerabilities create a table of risk, date discovered and describe what was recommended for the affected software.

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerabilities** | **Risk** | **Date Discovered** | **Recommendation** |
| Microsoft.NET CVE-2018-8292 Information Disclosure Vulnerability | Medium | 10/09/2018 | Block external access at the network boundary. |
| Microsoft Windows NTFS CVE-2018-8411 Local privilege Escalation Vulnerability | Medium | 10/09/2018 | Permit local access for trusted individuals only. Where possible, use restricted environment and restricted shells. |
| Microsoft Windows DNS CVE-2018-8320 Security Bypass Vulnerability | Medium | 10/09/2018 | Permit privileged access for trusted individuals only.Where possible, use restricted environment and restricted shells. |
| Microsoft Windows DirectX CVE-2018-8486 Information Disclosure Vulnerability | Medium | 10/09/2018 | Communicate sensitive information through secur means. |
| Microsoft Windows Kernel 'Win32k.sys' CVE-2018-8453 Local Privilege Escalation Vulnerability | Medium | 10/09/2018 | Permit privileged access for trusted individuals only.Where possible, use restricted environment and restricted shells. |