**Cybersecurity 401**

**Module 6 - Threat Modeling and Analysis**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Read 27 - Persistence**



**| Rodrigo Brasil 12/2023 |**

****

While no longer maintained by its original creator as of writing, PowerShell Empire has been forked many times and was used by nation state actors from 2015-2019. The PowerShell Empire project is now actively maintained by BC Security. As you read this article, take note of its original purpose as well as the tactical advantages offered to its users.

1. **What is one of the major advantages of PowerShell Empire?**
   1. Because powershell comes preinstalled with windows it makes it very powerful and it is its major advantage.
2. **What are some of the APT groups that have been known to use PS Empire and into which step of the Cyber Kill Chain does the use of PS Empire fall?**
   1. Some of the APT groups are APT32(OceanBuffalo), APT34(Oilrig) and APT41. The step on the cyber kill chain that PSEmpire stands is C2(Command and control)
3. **What are the four main components needed to pull off an attack using PS Empire?**
   1. The four main components needed to pull off an attack using PS Empire are: Listener, Agent, Module and Stager.