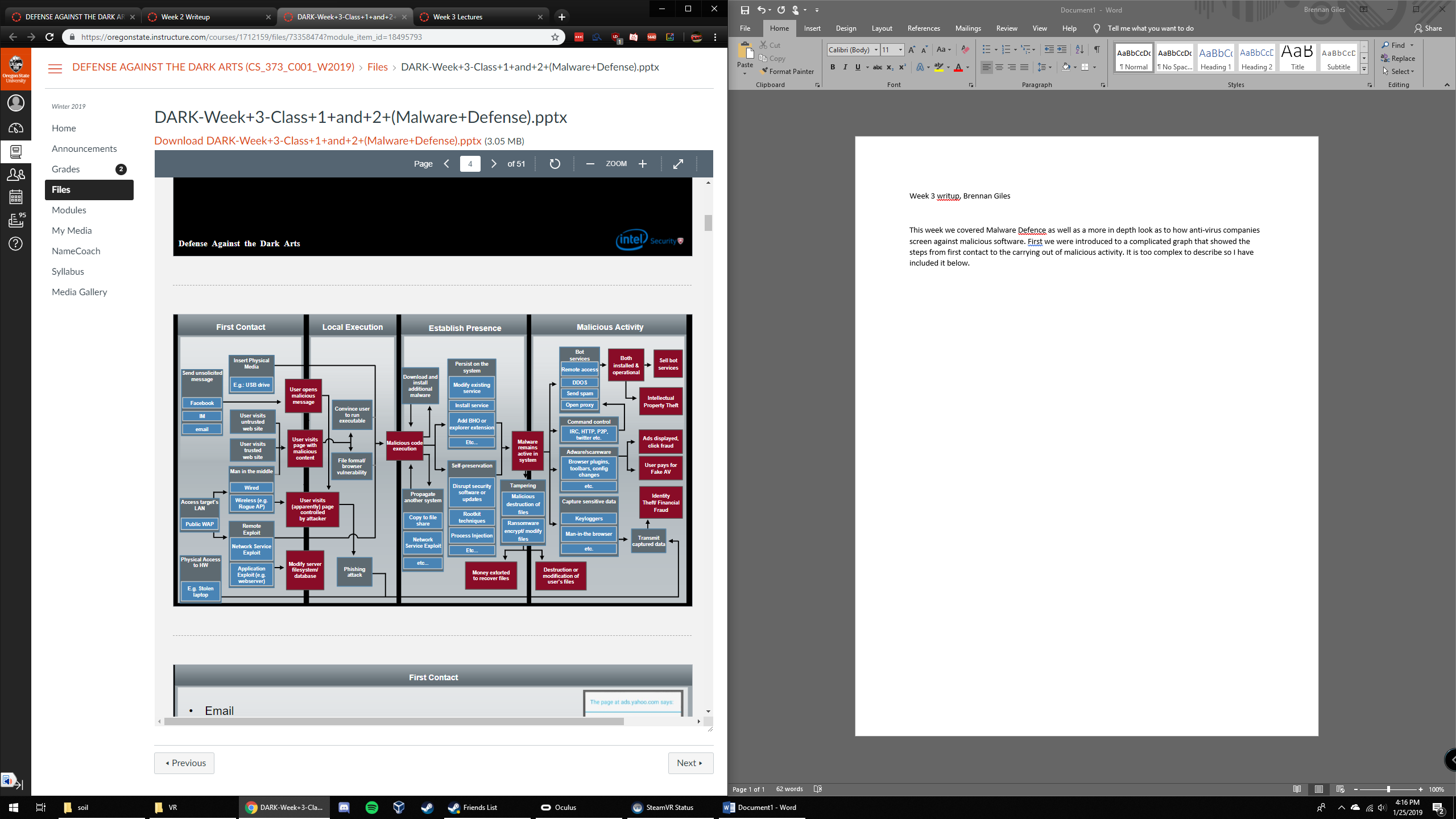
Week 3 writup, Brennan Giles

This week we covered Malware Defence as well as a more in depth look as to how anti-virus companies screen against malicious software. First we were introduced to a complicated graph that showed the steps from first contact to the carrying out of malicious activity. It is too complex to describe so I have included it below.



A lot of this information we had already gone over to be honest so I won’t repeat it, but a second in depth look is always useful. Next, we went further into malware defense and how the modern method is “layering” of defences. This means that first a firewall protects the network, then reputation/certs protect the host, then a host firewall protects the machine, and finally a host ips or antivirus protects control of the system. If a piece of malware gets past all these layers it gains control, however it needs to be able to circumvent all of these protections. Next YARA was introduced, which is specialized software for pattern matching malicious code. The idea is that the user can set “rules” and the program parses through data looking for those keywords. If it finds it, there is probably malicious code inside (as long as the code was properly labeled and identified). Kind of a random note, but I wanted to include that it is extremely common for delphi to be used when writing malicious code so keep an eye out for that language.