**LAB 3 - Malware Case Study**

Chris Fullerton

9/3/25

Course: CYBR-1100 Security Awareness

Week 3 Assignment

**Malware Type**

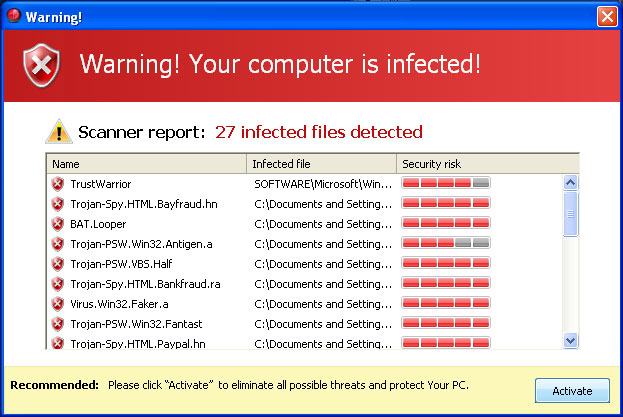
Virus is a software designed to harm or exploit a computer system, network, or user that is a type of malware that replicates itself by inserting its code into other programs to infect new hosts.

**Infection Method & symptom**

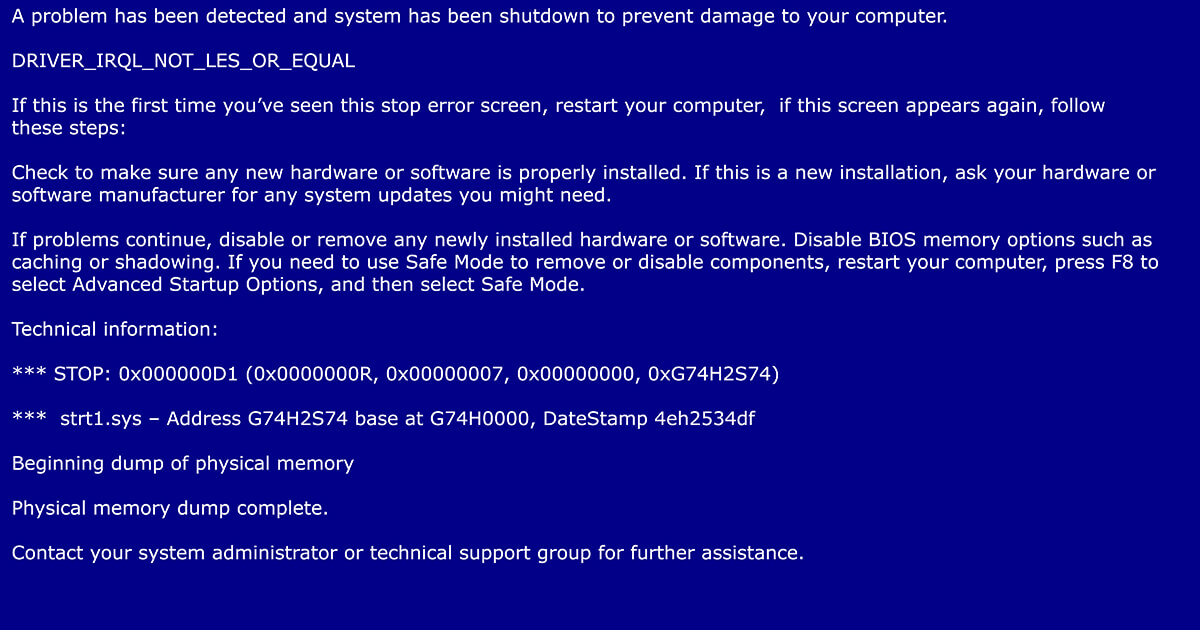
Viruses can be infected on your device by simply clicking on a link, or installing an untrusted program. Phishing is often used to trick users into installing viruses. When a virus does get installed users may not even know it, it would depend on the type of virus you would get. Some viruses will sit in the background and wait for you to enter in sensitive information or other viruses can bog down or crash your device all together.

**Evidence**

If you scan your device for viruses and indeed have them you likely will see something similar to the image below. Like mentioned above a lot of times you would not know if you had a virus so evidence can be hard to find.



If you had a virus that was catastrophic and indeed crashed or ruined your device it could look similar to the image below which is called the blue screen of death. This usually means your device is compromised.



**Defense and mitigation**

Three big defense or counter measures to ensure you don't get a virus is to make sure you always have an up to date virus detector downloaded. Second, you will always make sure your firewall is on and up to date. The third would be to make sure your device is always up, these updates usually always patch and fix vulnerabilities.

**Netcad Linkage**

This links to Netcad because netcad goes into detail about what to look for in Phishing attacks to try and get viruses installed into your device. The netcad will also show you how to prevent and inform on Virus detection.