Blue Team Lab

# Indicators

*You thought you had seen it all when it comes to malware but today is different. You are presented with a fresh sample, but it appears different from the others. Time to dissect, deobfuscate and detonate this sample just like all the others.*

*Reverse Engineering*

*Easy*

First comes identifying the bit of non-obfuscated code. I didn’t quite recognize it at first but some very smart searching of the “CreateObject” command brought me to believe it was visual basic script that was being used (it took a few guesses to get the spelling they wanted me to go with.

Oof, was really hoping for a “Decode” button. While looking at the code to figure out how to do this, I noticed that one of the strings was repeated but there were letters in between these repeats. I replaced the long string named Camtasia with nothing and got a new section of code. Looks to be PowerShell! Funny enough now I see there was a function for that at the bottom as well. Oops. Looks like I don’t quite understand how to find out class and method, so I’ll take a break and give it another attempt in the morning. Once decoded, some of the other answers were extremely obvious, so I filled those in as I saw them. I’ll have to devote some time to the time wasters though.