# Wykrywanie incydentów - lab 6

## Zadanie 1

1. **Wymień trzy funkcje AutoExec, które zostały wykorzystane.**
- AutoOpen
- Auto_Open
- Workobok_Open
2. **Jakie trzy funkcje (keywords) olevba wskazuje jako potencjalnie użyte do obfuskacji makra?**
- Chr Xor
- Hex
- Strings
3. **Z jakiej domeny makro próbuje pobrać plik exe? (domenę zapisz w bezpiecznym formacie)**
- http://imperialenergy/[.]ca/js/bin.exe

## Zadanie 2

1. **Podaj nazwę oraz lokalizację pliku .bat który tworzy makro.**
   %Temp%\d.bat
2. **Podaj adres IP oraz nazwę pliku, który próbuje pobrać powershell.**
   Nazwa: rs.txt
   Adres IP: 13.36.211.176
3. **Jak nazywa się strumień OLE zawierający to makro?**
   NewMacros
4. **Podaj rozmiar pliku vbaProject.bin (w KB).**
   34 KB

## Zadanie 3

1. **W którym pliku zlokalizowane jest makro?**
   sheet1.xml
2. **Podaj nazwy trzech plików wykonywalnych należących do tak zwanych „LOLBins" (https://lolbas-project.github.io), które wykorzystuje to makro.**
- csc.exe
- certutil.exe
- installutil.exe
3. **Podaj nazwę pliku z kodem C#, który próbuje pobrać makro.**
   tmp.cs