

1.What security protocol is being used for the communication with a malicious domain? (3 points)

**TLS 1.2**

2.What directory does the obfuscated PowerShell create? (Starting from \HOME\) (4 points)

**\HOME\Db\_bh30\Yf5be5g\**

3.What file is being downloaded (full name)? (4 points)

**A69S.dll**

4.What is used to execute the downloaded file? (3 points)

**Rundll32**

5.What is the domain name of the URI ending in ‘/6F2gd/’ (3 points)

**wm.mcdevelop.net**

6.Based on the analysis of the obfuscated code, what is the name of the malware? (3 points)

**Emotet**