**Macrerpreter**

Macrerpreter is an implant that spawns a meterpreter session on the victim’s computer. The implant is enabled by MITRE ATT&CK technique “Office Application Startup”. Social engineering techniques are utilized, and a victim is sent a malicious Word document. In this case, the Word document is called “Bank Statement” and has a blurred image of a bank statement – implying that the statement will be unblurred upon the enabling of macros. When the user chooses to enable macros, the AutoOpen macro is triggered, which downloads our malicious executable and spawns a meterpreter shell.

The execution technique used by Macrerpreter is the utilization of malicious Word macros. This technique is most commonly used by both the Silence and Codoso groups in conjunction with meterpreter shells.