**Задача**

Исследователю ВПО передали на исследование архивный файл (**CITIBANK TELEX REMITTANCE.rar**), содержащий необычный файл (**SWIFT COPY - MT-103.jse**), который получил по почте один из пользователей крупной компании. Пользователь сообщил, что специалисты ИБ его компании обнаружили на его компьютере, после запуска данного файла процесс с именем исполняемого файла: **UJHYTGD.exe,** который был идентифицирован как шпионское ВПО, а сам файл был значительно больше в размере, чем файл jse. Руководитель организации поставил задачу исследователю ВПО – установить URL с которого был загружен данный вредоносный файл и определить все возможные местоположения данного файла, после его загрузки из сети Интернет.

***(внимание – исследование файла следует проводить на виртуальной машине. Некоторые антивирусы определяют данные файлы и сам архив, как ВПО. Сам файл на сайте отсутствует, таким образом скрипт не сможет его загрузить и активировать)***