**Задача**

Руководитель подразделения ИБ одной из компаний получил письмо, подписанное предположительно одним из руководителей МЧС, содержащее архив с файлом «Graphik\_45.zip». Посчитав письмо легитимным, он сохранил файл архива и открыл файл «Graphik\_45.wsf». Позже, решив, что результат работы данного файла и сам файл выглядят подозрительно, так как при его запуске не открылся ожидаемый документ руководитель подразделения пригласил специалиста по ИБ для расследования инцидента. Установите, что происходит при открытии файла и запуске данного файла? Оцените вероятность заражения ПК руководителя подразделения ИБ, если на тот момент на его ПК был установлен антивирус Symantec Endpoint Protection. В качестве основного ответа к задаче приведите MD5 хеш URL’a на который переходит Internet Explorer, в случае успешного запуска данного файла, а также MD5-хеш команды и MD5-хеш параметров команды, запускающей извлеченный исполняемый файл ВПО, если известно, что имя учётной записи пользователя было: den.

Ответ:

При запуске данного скрипта из его кода извлекается сохраненный исполняемый файл вредоноса, который сохраняется в каталоге: «**Users\den\AppData\Local\Temp\**» и называется: «**OptimizationQueryDiagnosis.exe**».

Компьютер заражен не был (вероятность 0), так как скрипт не срабатывает на ПК в каталоге Program Files которых присутствуют каталоги зарубежных антивирусных компаний: Bit Defender, Norton, Symantec.

Браузер пытается открыть URL: **https://mchs.gov.ru/dokuments/grafik\_45**

MD5 1: **72ef1b43fcb16dd23644169d03fa30bb**

ВПО запускается с помощью программы: **rundll32.exe**

MD5 2: **13f43b565119f43f7155f96cafa8b05d**

Параметры запуска rundll32: **ieadvpack.dll,RegisterOCX C:\Windows\winhlp32.exe\..\..\Users\den\AppData\Local\Temp\OptimizationQueryDiagnosis.exe**

MD5 3: **21c5a9135b57311743187ff8915ebb3d**

***Внимание! При вычислении пути к исполняемому файлу ВПО система возвращает путь и именем учётной записи текущего пользователя, например: c:\Users\chser. Участники CTF должны заменить свое имя учётной записи на имя учётной записи, указанное в задании.***