Приложение 4 – Обозначения активностей в цепочке событий

 - Новый процесс

 - Автозагрузка

 - Новый сервис

 - Внедрение кода

 - Доступ к клавиатуре

 - Доступ к внедрению кода

 - Доступ к реестру автозагрузки

 - Извлечение исполняемого файла

 - Установлено интернет – соединение

 - Ожидание входящего подключения

 - Подключение к локальной сети

 - Попытка установки интернет – соединения (неудачно)

 - Перемещение важного файла

 - Открытие чужого исполняемого файла

 - Запись в чужой исполняемый файл (модификация)

 - Инфицирование чужого исполняемого файла (инжект кода в файл)

 - Открытие множества чужих исполняемых файлов

 - Запись в многие исполняемые файлы (массовая модификация)

 - Инфицирование многих чужих исполняемых файлов (массовый инжект кода в файлы)

 - Создание нового системного задания для планировщика задач

 - Установка исполняемого файла на самозапуск (через планировщик задач)

 - Подозрительный процесс вторгся в ЛЕГИТИМНЫЙ процесс (внедрение DLL)

 - Недоверенный процесс задерживает исполнение (возможно для обхода детекта)

 - Доступ к диску на низком уровне

 - Доступ на низком уровне ко многим дискам

 - Управление диском на низком уровне

 - Отслеживание ключа реестра

 - Идентификация уникальной инсталляции Windows

 - Идентификация уникального компьютера

 - Считывает настройки интернета

 - Попытка установки множества интернет-соединений

 - Запись на диск на низком уровне

 - Удаление чужого исполняемого файла

 - Удаление многих исполняемых файлов (массовое удаление)

 - Открытие важного файла

 - Открытие множества важных файлов

 - Модификация важного файла

 - Модификация множества важных файлов

 - Удаление важного файла

 - Удаление множества важных файлов

Отредактировать эту страницу