Приложение 2 – Список активностей (событий)

Название события	Название параметров активности
Автозагрузка	Раздел реестра
	Имя ключа
	Путь до запускаемой программы
	Процесс-инициатор автозапуска
Новый процесс	Файл нового процесса
	Командная строка
	Процесс-родитель
Новый сервис	Имя сервиса
	Путь до программы сервиса
	Процесс инициатор
Внедрение кода	Процесс-цель инжекции
	Процесс инициатор (инжектор)
Кейлоггер	Процесс-шпион
	Программа-жертва
	Лог-файл клавиш (файл-учетки)
Доступ к внедрению кода	Открываемый процесс

Название события	Название параметров активности
	Процесс-источник
Доступ к реестру автозагрузки	Процесс инициатор
	Название ключа реестра
Извлечение исполняемого файла	Процесс-создатель файла (дроппер)
	Созданный файл
Установлено интернет - соединение	Процесс инициатор соединения
	Удаленный адрес
	Удаленный порт
	Локальный порт
	Тип протокола
Ожидание входящего подключения	Процесс-инициатор ожидающий подключения
	Локальный порт
	Тип протокола
Попытка установки интернет- соединения (неудачно)	Процесс инициатор соединения
	Удаленный адрес
	Удаленный порт
	Локальный порт
	Тип протокола
Перемещение важного файла	Процесс инициатор важного файла
	Новое имя файла

Название события	Название параметров активности
	Старое имя файла
Открытие чужого исполняемого файла	Процесс инициатор
	Открываемый файл
Открытие множества других исполняемых файлов	Процесс-инициатор
	Количество файлов
	Директории
Запись в чужой исполняемый файл (модификация)	Процесс-инициатор
	Модифицированный файл
Запись в многие исполняемые файлы (массовая модификация)	Процесс-инициатор
	Количество файлов
	Типы файлов
	Директории
Инфицирование чужого исполняемого файла (инжект кода в файл)	Процесс-инициатор
	Инфицированный файл
Инфицирование многих чужих исполняемых файлов (массовый инжект кода в файлы)	Процесс-инициатор
	Количество файлов
	Типы файлов
	Директории
Создание нового системного задания для планировщика задач	Процесс-инициатор
	Имя задания в планировщике

Название события	Название параметров активности
Установка исполняемого файла на самозапуск (через планировщик задач)	Процесс-инициатор
	Объект установленный на самозапуск
	Имя задания в планировщике
	Время и дата запуска объекта
	Имя пользователя для задания
Подозрительный процесс вторгся в легитимный процесс (внедрение DLL)	Процесс-цель инжекции
	Процесс инициатор (инжектор)
	Внедренный файл DLL
Недоверенный процесс задерживает исполнение (возможно для обхода детекта)	Процесс инициатор
	Время задержки исполнения
	Метод задержки
	Имя системного объекта используемого для задержки
Доступ к диску на низком уровне	Процесс инициатор
	Тип доступа
	Имя диска
Доступ на низком уровне ко многим дискам	Процесс инициатор
	Тип доступа
	Типы дисков
	Количество дисков
Управление диском на низком уровне	Процесс инициатор

Название события	Название параметров активности
	Имя диска
	Тип операции с диском
	Код управления для драйвера
Отслеживание ключа реестра	Процесс инициатор
	Название ключа реестра
	Значение фильтра события
	Тип операций с ключом
Идентификация уникальной инсталляции Windows	Процесс инициатор
	Название ключа реестра
	Атрибут Windows (используемый для идентификации)
Идентификация уникального компьютера	Процесс инициатор
	Название ключа реестра
	Атрибут компьютера (используемый для идентификации)
Считывает настройки интернета	Процесс инициатор
	Название ключа реестра
	Настройка
Попытка установки множества интернет-соединений (перебор IP- адресов)	Процесс инициатор соединения
	Количество сетевых соединений
	Подсеть удаленных адресов

Название события	Название параметров активности
	Список удаленных портов
	Список локальных портов
	Типы протоколов
Запись на диск на низком уровне	Процесс инициатор
	Имя диска
	Позиция начала записи (смещение)
	Количество записанных байт
	Записанный текст (символы)
	Записанный сырой буфер (байты)