




Отчет динамического анализа

На странице динамического анализа отображаются результаты динамического анализа, проведенного на виртуальной машине среды исполнения.

Краткий отчет - показывает индикаторы потенциальных угроз и раскрывающийся список найденных активностей.







Краткий отчет

Детальный отчет

Цепочка событий

Логи производительности

Общая активность

Новый процесс

Файл нового процесса

\\SystemRoot\\System32\\Conhost.exe

C:\\Windows\\System32\\WScript.exe

Процесс-родитель

C:\\Windows\\System32\\cmd.exe

C:\\Windows\\System32\\cmd.exe

Модификация ОС (внедрение)

Внедрение кода

Процесс-цель инъекции

System

Процесс-инициатор (инжектор)

C:\\Windows\\System32\\uhclient.exe

Сбор информации о хосте

Идентификация уникального компьютера

Атрибут компьютера (используемый для идентификации)

Имя компьютера

Имя компьютера

Криптографический идентификатор компьютера (GUID - привязка к аппаратной части)


Процесс-инициатор

\\SystemRoot\\System32\\Conhost.exe

C:\\Windows\\System32\\WScript.exe

C:\\Windows\\System32\\WScript.exe

Рис. 15 – Отчет по динамическому анализу



Отредактировать эту страницу