**Отчет по анализу дампа оперативной памяти**

1. Постановка задачи  
В результате несанкционированной инициализации съемного накопителя в системе было запущено вредоносное программное обеспечение (ПО) под именем project.exe. ПО использовало Windows API для получения сведений о системе. На основании дампа оперативной памяти требовалось:

Найти название использованной Windows API функции.

Установить её назначение и результат выполнения.

Найти в дампе конкретный результат (значение) её вызова, который и является ключом для задания.

2. Ход анализа

2.1. Анализ процесса и используемых API  
Был загружен предоставленный дамп оперативной памяти. С использованием методов анализа памяти (Volatility Framework) был идентифицирован целевой процесс project.exe (PID: 3820). В его адресном пространстве был проведен анализ импортируемых функций и строк, что позволило выявить использование функции GetAdaptersInfo из библиотеки iphlpapi.dll.

2.2. Исследование функции GetAdaptersInfo  
Справка из открытых источников (официальная документация Microsoft) показала следующее:

Назначение: Функция GetAdaptersInfo предназначена для получения информации о конфигурации сетевых адаптеров на компьютере.

Результат выполнения: Функция заполняет буфер структурой IP\_ADAPTER\_INFO, которая содержит подробные данные о каждом сетевом адаптере, включая:

Описание адаптера.

Физический (MAC-) адрес адаптера.

IP-адрес, маску подсети, адрес шлюза.

Адреса DHCP- и WINS-серверов.  
Было сделано предположение, что целью вредоносного ПО был сбор уникальных идентификаторов системы, таких как MAC-адрес.

2.3. Поиск результата выполнения функции в памяти  
В рамках процесса project.exe был проведен поиск артефактов, соответствующих структуре данных, возвращаемой функцией GetAdaptersInfo. В памяти процесса был обнаружен буфер, содержащий результат успешного вызова данной функции. Анализ этого буфера позволил извлечь значение MAC-адреса сетевого адаптера.

3. Результаты и выводы

Использованная Windows API функция: GetAdaptersInfo.

Назначение функции: Получение данных о сетевых адаптерах системы.

Ключевой результат выполнения функции (Найденный ключ): **50A4C8D133A6**.

Вывод: Вирус программа project.exe успешно выполнила функцию GetAdaptersInfo с целью сбора конфиденциальной информации о системе, а именно — уникального MAC-адреса сетевого адаптера 50A4C8D133A6. Данный идентификатор может быть использован для отслеживания системы или привязки к ней другой вредоносной активности.