Результаты расследования инцидента в задании Модуля D

Executive Summary

Высокоуровневое описание инцидента. Здесь представлена информация, которая представляет наибольшую важность для исполнительных руководителей компании без указания конкретных технических подробностей. Данный раздел должен содержать:

1. Временные рамки инцидента

2. Вектор(а) атаки

3. Высокоуровневое описание последовательности атаки

4. ВПО и инструменты, которые были использованы в процессе атаки (без конкретного описания технических деталей)

5. Какие цели были поставлены злоумышленниками и какие результаты были достигнуты при атаке Объекты исследования

Объекты исследования

Название объекта исследования	Описание объекта исследования
traffic.pcap	Дамп сетевого трафика Wireshark

Результаты исследования

Данный раздел содержит технические детали инцидента.

Временные рамки инцидента

В таблице данного раздела участникам необходимо привести конкретные события на скомпрометированных системах.

Ключевые Данные

Атакующий:
Ip:194.180.191.64
Role: Сервер управления

Жертва:
Ip: 10.11.26.183
Name: DESKTOP-B8TQK49)
MAC: d0:57:7b:ce:fc:8b
Host: nemotoads.health

Контроллер домена:
Ip:10.11.26.3
Host: nemotodes-dc.nemotodes.health
Gate: 10.11.26.1 (Cisco)

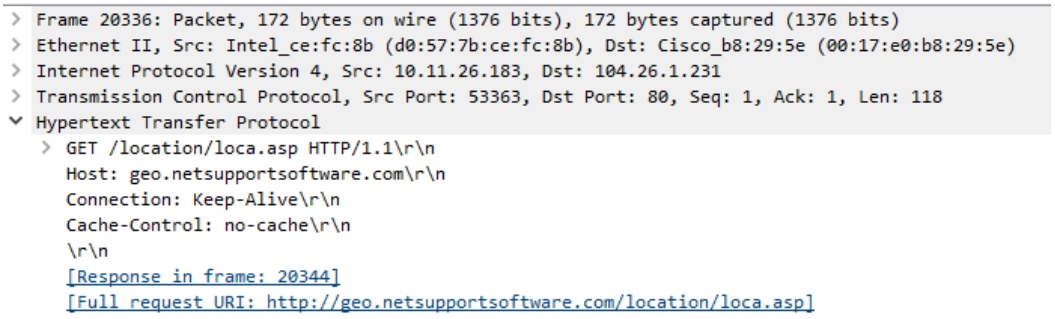
Хронология инцидента

Этап 1: Проверка геолокации и окружения

Сразу после стандартных проверок подключения к Microsoft (NCSI), вредоносное ПО выполнило проверку местоположения зараженного компьютера. Это стандартное поведение для NetSupport RAT, чтобы определить, стоит ли атаковать данную цель (например, некоторые группировки избегают атак на страны СНГ).

Событие: DNS-запрос к `geo.netsupportsoftware.com`.

В пакете №20336 (время `67.28`) жертва отправляет HTTP GET запрос: `GET /location/loca.asp HTTP/1.1` на IP `104.26.1.231`.



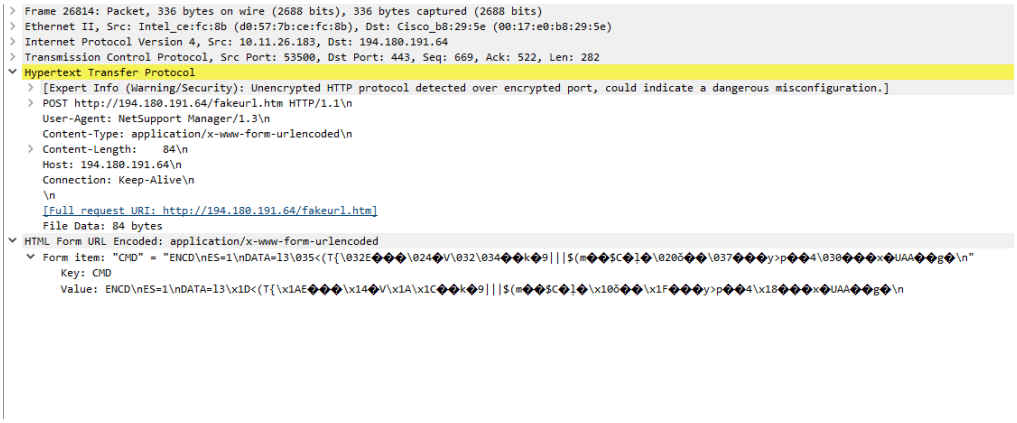
Это подтверждает использование именно программного обеспечения NetSupport.

Этап 2: Соединение с командным центром

Сразу после проверки локации, вредонос инициировал связь с сервером злоумышленника.

Время начала: `3050.859267` (пакет №26814) и ранее в пакете №20340.

Запрос: `POST` http://194.180.191.64/fakeurl.htm.



Анализ URL: Путь `/fakeurl.htm` является жестким индикатором (сигнатурой) взломанной версии NetSupport RAT. Легитимный софт обычно не использует такие пути. Данные передаются методом `POST` с типом контента `application/x-www-form-urlencoded`. В теле запроса обычно содержатся данные о системе (имя пользователя, версия ОС) или результаты выполнения команд. Ответ сервера `200 OK` подтверждает, что злоумышленник успешно получил данные.

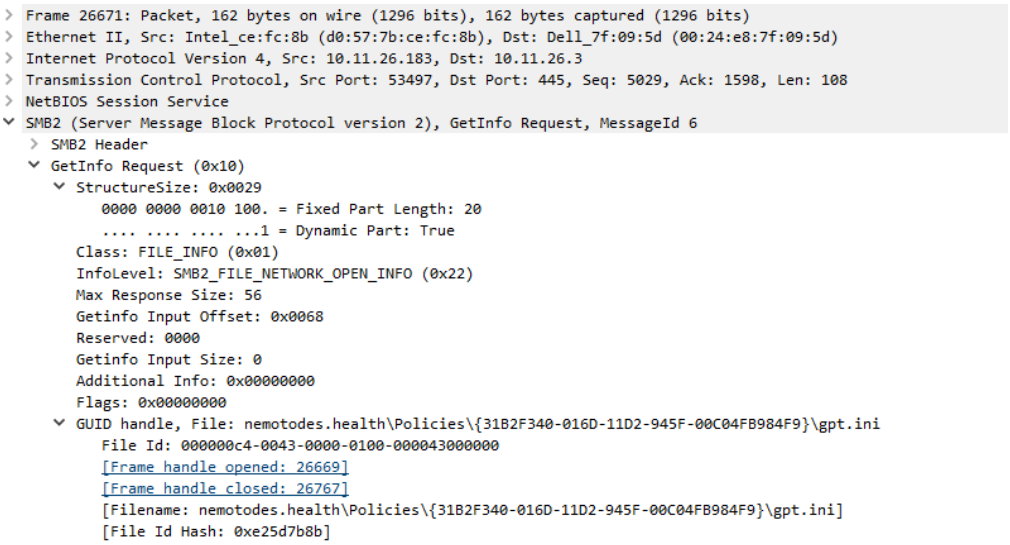
Этап 3: Внутренняя активность

Параллельно с внешней связью, зараженный хост ведет подозрительно активный обмен данными с контроллером домена `10.11.26.3`:

SMB (порт 445): Попытки доступа к файловым шарам `\\NEMOTODES-DC\IPC$` и `\\NEMOTODES-DC\Shared_Files`.

LDAP: Множественные запросы к Active Directory (поиск политик, групп пользователей).

Это может указывать на то, что хакер или автоматический скрипт пытается собрать информацию о правах доступа или распространиться на контроллер домена (Lateral Movement). Например, попытка доступа к gpt.ini, который отвечает за групповые политики:



Заключение и рекомендации

Что произошло:

Компьютер `DESKTOP-B8TQK49` был заражен, вредоносное ПО установило постоянный канал связи с сервером `194.180.191.64`, используя маскировку под легитимный трафик HTTP, и начало передачу данных.

Рекомендуемые действия:

1. **Изоляция:** Отключить хост `10.11.26.183` от локальной сети.
2. **Блокировка:** Добавить IP `194.180.191.64` и URL-паттерн `*/fakeurl.htm` в черный список на шлюзе.
3. **Анализ:** Проверить контроллер домена `10.11.26.3` на наличие подозрительных авторизаций с зараженного хоста.
4. **Очистка:** На зараженной машине необходимо найти процессы `client32.exe` которые часто маскируются в папках `%APPDATA%`.