

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.

```
> Frame 20336: Packet, 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Cisco_b8:29:5e (00:17:e0:b8:29:5e)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 104.26.1.231
> Transmission Control Protocol, Src Port: 53363, Dst Port: 80, Seq: 1, Ack: 1, Len: 118
▼ Hypertext Transfer Protocol
  > GET /location/loca.asp HTTP/1.1\r\n
    Host: geo.netsupportsoftware.com\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Response in frame: 20344]
    [Full request URI: http://geo.netsupportsoftware.com/location/loca.asp]
```

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>.

```
> Frame 26814: Packet, 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Cisco_b8:29:5e (00:17:e0:b8:29:5e)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 194.180.191.64
> Transmission Control Protocol, Src Port: 53500, Dst Port: 443, Seq: 669, Ack: 522, Len: 282
+ Hypertext Transfer Protocol
  > [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
  > POST http://194.180.191.64/fakeurl.htm HTTP/1.1\n
    User-Agent: NetSupport Manager/1.3\n
    Content-Type: application/x-www-form-urlencoded\n
  > Content-Length:      84\n
    Host: 194.180.191.64\n
    Connection: Keep-Alive\n
    \n
    [Full request URI: http://194.180.191.64/fakeurl.htm]
    File Data: 84 bytes
+ HTML Form URL Encoded: application/x-www-form-urlencoded
  + Form item: "CMD" = "ENC(nES=1;nDATA=13\035<(T{032E00000240V103203400k09||$(m05C0102080003700yypp04030000xUAA00g0ln\"
    Key: CMD
    Value: ENC(nES=1;nDATA=13\xID<(T{xIAE0000xI40V1xAIXc00k09||$(m05C010x18000xIF00yypp040x18000xUAA00g0ln
```

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:

```
> Frame 26671: Packet, 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
> Ethernet II, Src: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
> Internet Protocol Version 4, Src: 10.11.26.183, Dst: 10.11.26.3
> Transmission Control Protocol, Src Port: 53497, Dst Port: 445, Seq: 5029, Ack: 1598, Len: 108
> NetBIOS Session Service
▼ SMB2 (Server Message Block Protocol version 2), GetInfo Request, MessageId 6
  > SMB2 Header
  ▼ GetInfo Request (0x10)
    ▼ StructureSize: 0x0029
      0000 0000 0010 100. = Fixed Part Length: 20
      .... .... .... 1 = Dynamic Part: True
    Class: FILE_INFO (0x01)
    InfoLevel: SMB2_FILE_NETWORK_OPEN_INFO (0x22)
    Max Response Size: 56
    Getinfo Input Offset: 0x0068
    Reserved: 0000
    Getinfo Input Size: 0
    Additional Info: 0x00000000
    Flags: 0x00000000
  ▼ GUID handle, File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
    File Id: 000000c4-0043-0000-0100-000043000000
    [Frame handle opened: 26669]
    [Frame handle closed: 26767]
    [Filename: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini]
    [File Id Hash: 0xe25d7b8b]
```

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%.