

Отчет Модуль D – «Цифровая криминалистика»

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

В период с 26 ноября 2024 04:49:38 UTC по 26 ноября 2024 05:43:58 UTC рабочая станция DESKTOP-B8TQK49 (10.11.26.183), находящаяся в домене nemotoads.health, была скомпрометирована вредоносным ПО типа Remote Access Tool (RAT) – NetSupport Manager 1.3. Злоумышленник получил и поддерживает полноценный удалённый доступ к системе. На момент захвата дампа уже происходила активная связь с командным сервером (C2) по адресу 194.180.191.64 через порт 443 (plaintext HTTP внутри TLS-туннеля). Вектор атаки похож на загрузку через фальшивое обновление браузера (кампания типа SocGhosh/FakeUpdate). Предположительная суть атаки по таблице MITRE ATT&CK – T1219: ПО для удаленного доступа для дальнейшей компрометации домена.

Таблица 1 – Объекты исследования

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

Исследование проводилось с помощью Wireshark и Zui.

Результаты исследования

Данный раздел содержит технические детали инцидента.

Временные рамки инцидента

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

Таблица 2 – временные рамки инцидента

Дата и время события (UTC)	Краткое описание события
2024-11-26 04:49:38.458	Проверка интернет-подключения (NCSI на www.msftconnecttest.com)
2024-11-26 04:49:38 – 04:49:41	Активная сетевая разведка: LDAP SRV, WPAD, mDNS, LLMNR, NBTNS, SSDP
2024-11-26 04:49:39 – 04:49:41	Подключение к доменному контроллеру (10.11.26.3:389), чтение SYSVOL и GPO
2024-11-26 05:40:28	Установление TCP-соединения с C2 194.180.191.64:443
2024-11-26 05:41:29.372	Первый NetSupport RAT check-in (POST /fakeurl.htm, User-Agent: NetSupport Manager/1.3)
2024-11-26 05:41:29 – 05:43:58	Регулярные heartbeat-запросы примерно каждые 60 секунд (больше 5 зафиксированных POST)
2024-11-26 05:43:58	Завершение захвата дампа

Вектор атаки и подтверждающая информация

В дампе отсутствует (мной не найден) момент первоначального заражения, но характерные признаки (User-Agent NetSupport Manager/1.3 и типичный C2-трафик) однозначно указывают на кампании типа SocGhosh или FakeUpdate. Пользователь, скорее всего, перешёл по вредоносной рекламе или фишинговой ссылке и скачал «обновление браузера», которое запустило NetSupport RAT.

Далее приведены скриншоты, подтверждающие данный вектор.

```

event_type: alert (2),
ts: 2024-11-26T04:50:46.046139Z,
src_ip: 10.11.26.183,
src_port: 53362 (port=(uint16)),
dest_ip: 194.180.191.64,
dest_port: 443 (port=(uint16)),
vlan: null ([uint16]),
proto: "TCP",
app_proto: "http",
alert: √ {
  severity: 2 (uint16),
  signature: "ET POLICY HTTP traffic on port 443 (POST)",
  category: "Potentially Bad Traffic",
  action: "allowed",
  signature_id: 2013926 (uint64),
  gid: 1 (uint64),

event_type: alert (3),
ts: 2024-11-26T04:50:46.046139Z,
src_ip: 10.11.26.183,
src_port: 53362 (port=(uint16)),
dest_ip: 194.180.191.64,
dest_port: 443 (port=(uint16)),
vlan: null ([uint16]),
proto: "TCP",
app_proto: "http",
alert: √ {
  severity: 3 (uint16),
  signature: "ET INFO NetSupport Remote Admin Checkin",
  category: "Misc activity",
  action: "allowed",
  signature_id: 2035892 (uint64),
  gid: 1 (uint64),

```

Рисунки 1-2 Alerts от Suricata, подтверждающие опасное удаленное подключение

Описание последовательности атаки и подтверждающая информация

Представим этот раздел в виде таблиц и под ними добавлю подкрепляющие достоверность сказанного скриншоты.

Таблица 3 – последовательность атаки с тактиками и техниками MITRE (с сайта mitre.ptsecurity.com)

Тактика	Техника	ID	Комментарий
Начальный доступ	Drive-by Compromise	T1189	фальшивое обновление браузера (SocGhosh)?
Выполнение	Легитимное ПО как malware (Masquerading)	T1218	Запуск настоящего NetSupport Manager в роли RAT
Обнаружение	Обнаружение сетевой конфигурации	T1016	WPAD, mDNS, LLMNR, NBTNS, SSDP
Обнаружение	Обнаружение доменного контроллера	T1069.002	LDAP SRV-запросы _ldap._tcp
Обнаружение	Обнаружение удалённой системы	T1018	Попытки разрешения имён через LLMNR/NBTNS
Закрепление	Использование легитимного ПО для удалённого доступа	T1219	NetSupport Manager обеспечивает постоянный доступ
Командование и управление (C2)	Веб-протоколы	T1071.001	HTTP POST на порту 443 (plaintext внутри)
Командование и управление (C2)	Шифрованный канал — асимметричный	T1573.002	Трафик идёт на 443, но без TLS — маскировка
Командование и управление (C2)	Нестандартный порт	T1572	Использование порта 443 для HTTP-трафика

```
_path: http,
ts: 2024-11-26T04:49:38.525014Z,
uid: "CC00ILVAiCNmWUUh3",
id: > {orig_h: 10.11.26.183, orig_p: 53279 (port=(uint16)), resp_h: 104.117.247.184, resp_p: 80 (port=(uint16))},
trans_depth: 1 (uint64),
method: "GET",
host: "www.msftconnecttest.com",
uri: "/connecttest.txt",
referrer: null,
version: "1.1",
user_agent: "Microsoft NCSI",
origin: null,
request_body_len: 0 (uint64),
```

Рисунок 3 – стандартная проверка коннекта

```

_path: dns,
ts: 2024-11-26T04:49:38.918598Z,
uid: "CK5X0v3QicvyPTyuoj",
id: > {orig_h: 10.11.26.183, orig_p: 55542 (port=(uint16)), resp_h: 10.11.26.3, resp_p: 53 (port=(uint16))},
proto: "udp" (zenum),
trans_id: 15180 (uint64),
rtt: 509us,
query: "_ldap._tcp.default-first-site-name._sites.nemotoads.health",
qclass: 1 (uint64),
qclass_name: "C_INTERNET",
qtype: 33 (uint64),
qtype_name: "SRV",
rcode: 0 (uint64),
rcode_name: "NOERROR",

```

Рисунок 4 – стандартный запрос для начала получения GPO

```

_path: dce_rpc,
ts: 2024-11-26T04:49:55.587339Z,
uid: "Cng6U334Y5zodh0i4f",
id: > {orig_h: 10.11.26.183, orig_p: 53291 (port=(uint16)), resp_h: 10.11.26.3, resp_p: 49671 (port=(uint16))},
rtt: 361us,
named_pipe: "49671",
endpoint: "drsuapi",
operation: "DRSCrackNames"

{
  _path: dce_rpc,
  ts: 2024-11-26T04:49:57.435524Z,
  uid: "ChSVW721xqvjD6qUX4",
  id: > {orig_h: 10.11.26.183, orig_p: 53304 (port=(uint16)), resp_h: 10.11.26.3, resp_p: 49671 (port=(uint16))},
  rtt: 206us,
  named_pipe: "49671",
  endpoint: "drsuapi",
  operation: "DRSUnbind"
}

```

Рисунок 5-6 – легитимный в данном случае трафик

```

_path: http,
ts: 2024-11-26T05:00:48.022865Z,
uid: "CNAAdqJ3kYU3phUuBXg",
id: > {orig_h: 10.11.26.183, orig_p: 53362 (port=(uint16)), resp_h: 194.180.191.64, resp_p: 443 (port=(uint16))},
trans_depth: 14 (uint64),
method: "POST",
host: "194.180.191.64",
uri: "http://194.180.191.64/fakeurl.htm",
referrer: null,
version: null,
user_agent: "NetSupport Manager/1.3",
origin: null,
request_body_len: 36 (uint64),
response_body_len: 0 (uint64),
status_code: null.

```

Рисунок 7 – Подтверждение получения легитимного ПО, которое будет использовано для атаки

```
id: > {orig_h: 10.11.26.183, orig_p: 53362 (port=(uint16)), resp_h: 194.180.191.64, resp_p: 443 (port=(uint16))},
source: "HTTP",
depth: 0 (uint64),
analyzers: > |["MD5", "SHA1"]|,
mime_type: "text/plain",
filename: null,
duration: 0s,
local_orig: true,
is_orig: true,
seen_bytes: 36 (uint64),
total_bytes: 36 (uint64),
missing_bytes: 0 (uint64),
overflow_bytes: 0 (uint64),
timedout: false,
parent_fuid: null,
md5: "d1f800d92f9783c66efbc5c6d36085bd",
```

Рисунок 8 – тело запроса типа files (определено Zui), поддерживающего коннект с ip из IOC

```
_path: dns,
ts: 2024-11-26T05:01:57.771757Z,
uid: "CKRo1342n3E4Fx90Lb",
id: > {orig_h: 10.11.26.183, orig_p: 51810 (port=(uint16)), resp_h: 10.11.26.3, resp_p: 53 (port=(uint16))},
proto: "udp" (zenum),
trans_id: 41710 (uint64),
rtt: null,
query: "wpad.nemotoads.health",
qclass: 1 (uint64),
qclass_name: "C_INTERNET",
qtype: 1 (uint64),
qtype_name: "A",
rcode: 3 (uint64),
rcode_name: "NXDOMAIN",

_path: dns,
ts: 2024-11-26T05:01:57.772258Z,
uid: "CKRo1342n3E4Fx90Lb",
id: > {orig_h: 10.11.26.183, orig_p: 51810 (port=(uint16)), resp_h: 10.11.26.3, resp_p: 53 (port=(uint16))},
proto: "udp" (zenum),
trans_id: 45643 (uint64),
rtt: null,
query: "wpad.mshome.net",
qclass: 1 (uint64),
qclass_name: "C_INTERNET",
qtype: 1 (uint64),
qtype_name: "A",
rcode: 3 (uint64),
rcode_name: "NXDOMAIN",
```

Рисунки 9-10 – легитимные wpad-запросы, показывающие, что прокси не настроен

20348 67.889917	10.11.26.183	194.180.191.64	HTTP	328 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
20350 68.291089	10.11.26.183	194.180.191.64	HTTP	336 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
20572 128.463544	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21145 188.645216	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21153 248.801955	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21246 308.968954	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21295 369.027534	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21337 429.088220	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21352 489.150466	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21364 549.304894	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21415 609.360011	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21608 669.564727	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)
21708 729.860051	10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1	(application/x-www-form-urlencoded)

Рисунок 11 – множественные http запросы на сайт из ИОС

Таблица 4 – алерты от Suricata (взято из Zui)

Время	Alert	Категория	Комментарий
2024-11-26 04:49:38.573	ET INFO Microsoft Connection Test	Misc activity	Обычная проверка NCSI
2024-11-26 05:41:29.372	ET POLICY HTTP traffic on port 443 (POST)	Potentially Bad Traffic	Plaintext HTTP внутри порта 443
2024-11-26 05:41:29.372	ET INFO NetSupport Remote Admin Checkin	Misc activity	Подтверждение NetSupport RAT
2024-11-26 05:42:29.528	ET POLICY HTTP traffic on port 443 (POST)	Potentially Bad Traffic	Повторный POST
2024-11-26 05:42:29.528	ET INFO NetSupport Remote Admin Checkin	Misc activity	Повторный check-in
2024-11-26 05:43:29.682	ET POLICY HTTP traffic on port 443 (POST)	Potentially Bad Traffic	-
2024-11-26 05:43:29.682	ET POLICY HTTP traffic on port 443 (POST)	Misc activity	-
2024-11-26 05:43:58.109	ET POLICY HTTP traffic on port 443 (POST)	Potentially Bad Traffic	-
2024-11-26 05:43:58.109	ET INFO NetSupport Remote Admin Checkin	Misc activity	Последний зафиксированный heartbeat

```
event_type: alert (2),
ts: 2024-11-26T05:42:29.52877Z,
src_ip: 10.11.26.183,
src_port: 53500 (port=(uint16)),
dest_ip: 194.180.191.64,
dest_port: 443 (port=(uint16)),
vlan: null ([uint16]),
proto: "TCP",
app_proto: "http",
alert: √ {
  severity: 2 (uint16),
  signature: "ET POLICY HTTP traffic on port 443 (POST)",
  category: "Potentially Bad Traffic",
  action: "allowed",

  metadata: √ {
    signature_severity: > ["Informational"],
    former_category: null ([string]),
    attack_target: > ["Client_Endpoint"],
    deployment: > ["Perimeter"],
    affected_product: null ([string]),
    created_at: > ["2011_11_18"],
    performance_impact: null ([string]),
    updated_at: > ["2024_03_12"],
    malware_family: null ([string]),
    tag: null ([string]),
    confidence: > ["High"],
    tls_state: > ["plaintext"]
```

Рисунок 12-13 – пример алерта

```
event_type: alert (2),
ts: 2024-11-26T05:00:48.022865Z,
src_ip: 10.11.26.183,
src_port: 53362 (port=(uint16)),
dest_ip: 194.180.191.64,
dest_port: 443 (port=(uint16)),
vlan: null ([uint16]),
proto: "TCP",
app_proto: "http",
alert: {
  severity: 2 (uint16),
  signature: "ET POLICY HTTP traffic on port 443 (POST)",
  category: "Potentially Bad Traffic",
  action: "allowed",
```

Рисунок 14 – Пример алерта

Индикаторы компрометации (ИОС)

Файловые индикаторы компрометации (shasum файлов, связанных с атакой; пути закрепления ВПО)

Таблица 5 – ИОС файлов

Тип	Значение	Комментарий
User-Agent	NetSupport Manager/1.3	Во всех запросах к C2
URI	http://194.180.191.64/fakeurl.htm	Фиктивный путь
MD5 (heartbeat)	d1f800d92f9783c66efbc5c6d36085bd	36-байтовый POST
SHA1 (heartbeat)	05542bc16e69e6cd6a14db1ac61443d91e98d99d	

Сетевые индикаторы компрометации (IP адрес(а) злоумышленника)

194.180.191.64 хостинг атакующих

10.11.26.183 скомпрометированный хост домена (он же DESKTOP-B8TQK49)

Вывод

В доменной среде RAT на одной рабочей станции – это потенциальный доступ ко всему домену (латеральное движение, кража хэшей из LSASS, спрей паролей и т.д.). Один заражённый хост – угроза всей инфраструктуре, поэтому данный вектор весьма опасен. Также несмотря на наличие DCE RPC drsuapi, атаку DCSync подтвердить нельзя из-за отсутствия операции DRSGetNCChanges. Основной угрозой является NetSupport Manager RAT, который уже имеет точку опоры в доменной среде nemotoads.health