Traffic Analysis

Executive Summary:

Approximately at around 00:11 UTC, 15.08.2024 on Thursday, a Windows host was infected with WarmCookie malware.

Victim Details:

- Host Name: DESKTOP-H8ALZBV
- IP Address: 10.8.15.133
- MAC Address: 00:1c:bf:03:54:82
- Windows user account name: plucero

Indicators of Compromise (IOCs):

ZIP download:

```
104.21.55.70:80 – quote.checkfedexexp.com – GET /managements?
16553a25e45250a41fd5&endeds=MIGpq&JStx=59bf050d37df88a9-
ade43358-eaa1220b-0571422b-0f33e6aa150e86bafd0ed4&Ld=
9d7502d88d752a27b1d00587309184b5a215
```

Follow-up download (unknown content):

```
172.67.170.169:443 – https://business.checkfedexexp.com/data-
privacy?zj=ZzqRKxVRQ&pOd=GEokiOXFwH&sourcedp=tQMQJlIo&Tfocont
ent=IxGTZjXqxJ&Jr_cid=9464552&
```

DLL download:

```
http://72.5.43.29/data/0f60a3e7baecf2748b1c8183ed37d1e4
```

POST-infection traffic:

```
72.5.43.29:80 – 72.5.43.29 - POST /
72.5.43.29:80 – 72.5.43.29 - GET /
```

Downloaded ZIP archive SHA256 hash:

```
798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5
File size: 2,767,804 bytes
File name: Invoice 876597035_003.zip
```

Extracted JS file SHA256 hash:

```
dab98819d1d7677a60f5d06be210d45b74ae5fd8cf0c24ec1b3766e25ce6dc2c
File size: 6,990,020 bytes
File name: Invoice-876597035-003-8331775-8334138.js
```

Downloaded DLL file SHA256 hash

b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6
File size: 159,232 bytes
File type: PE32+ executable (DLL) (GUI) x86-64, for MS Windows