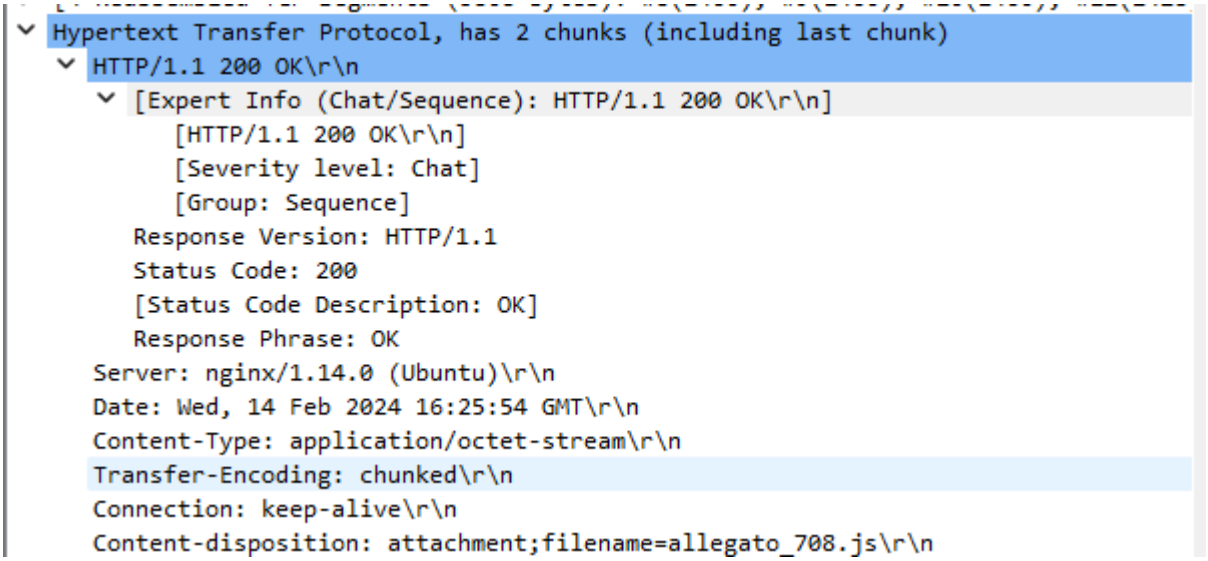
DanaBot_allunell

1.- ¿Qué dirección IP utilizó el atacante durante el acceso inicial?

```
62.173.142.148
```

2.- ¿Cómo se llama el archivo malicioso utilizado para el acceso inicial?

```
allegato_708.js
```



3.- ¿Cuál es el hash SHA-256 del archivo malicioso utilizado para el acceso inicial?

CREDITOS A AITOR SEGURA.

```
847B4AD90B1DABA2D9117A8E05776F3F902DDA593FB1252289538ACF476C4268
```

General Info

Add for printing

File name: allegato_708.js

Full analysis: https://app.any.run/tasks/a886894d-8ae4-4d59-a990-b59536885da8

Verdict: Malicious activity

Threats: Danabot Loader Stealer

Danabot is an advanced banking Trojan malware that was designed to steal financial information from victims. Out of the Trojans in the wild, this is one of the most advanced thanks to the modular design and a complex delivery method.

Malware Trends Tracker >>>

Analysis date: February 14, 2024 at 23:37:03

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags: loader danabot danabot-unpacked stealer

Indicators:

MIME: text/plain

File info: ASCII text, with very long lines (5558), with no line terminators

MD5: 5DAF53BF848BB4CDA008A655BDECF425

SHA1: 422EDA5A133D4BD324C634F113639A57C38BB552

SHA256: 847B4AD90B1DABA2D9117A8E05776F3F902DDA593FB1252289538ACF476C4268

SSDEEP: 96:j1Xp6Fi8ComWlyo5kxb2mRWcxHnLVRmqq4mAP0JEp7USUO5ip5iW33KlKXFd18eH:D6FismQVmamRVHLVwtKP8KK6uGiut3W

4.- ¿Qué proceso se utilizó para ejecutar el archivo malicioso?

```
wscript.exe
```

Behavior activities

Add for printing

MALICIOUS

Creates internet connection object (SCRIPT)
- wscript.exe (PID: 3672)

Unusual connection from system programs
- wscript.exe (PID: 3672)
- rundll32.exe (PID: 3304)

Opens an HTTP connection (SCRIPT)
- wscript.exe (PID: 3672)

Sends HTTP request (SCRIPT)
- wscript.exe (PID: 3672)

Gets path to any of the special folders (SCRIPT)
- wscript.exe (PID: 3672)

SUSPICIOUS

Writes binary data to a Stream object (SCRIPT)
- wscript.exe (PID: 3672)

Creates a Stream, which may work with files, input/output devices, pipes, or TCP/IP sockets (SCRIPT)
- wscript.exe (PID: 3672)

Creates FileSystem object to access computer's file system (SCRIPT)
- wscript.exe (PID: 3672)

Reads the Internet Settings
- wscript.exe (PID: 3672)
- rundll32.exe (PID: 3304)

INFO

Checks proxy server information
- wscript.exe (PID: 3672)
- rundll32.exe (PID: 3304)

Reads Windows Product ID
- rundll32.exe (PID: 3304)

Create files in a temporary directory
- rundll32.exe (PID: 3304)

5.- ¿Cuál es la extensión del segundo archivo malicioso utilizado por el atacante?

```
.dll
```

Dropped files

PID	Process	Filename	Type
3304	rundll32.exe	C:\Users\admin\AppData\Local\Temp\Peeopqps	sqlite
		MD5: 2E0913940F10B470636C82686F0F414E	**SHA256:** 5E76AC5A19DF3AD6723E3CED14663944C1506C5B4580FB9AA4619B36AFDECD84
3672	wscript.exe	C:\Users\admin\AppData\Local\Temp\JffleeTicl.dll	executable
		MD5: E758E07113016ACA55D9EDA2B0FFEEBE	**SHA256:** 2597322A49A6252445CA4C8D713320B238113B3B8FD8A2D6FC1088A5934CEE0E
3304	rundll32.exe	C:\Users\admin\AppData\Local\Temp\Pqrayhopiidyqh	binary
		MD5: 03EF1C0012EE77CDA2C2CB36DFBDA123	**SHA256:** 800D734016D8FBCDE263D8CD2411167406C544FC090A5DCBD2D374CABF918B86
3304	rundll32.exe	C:\Users\admin\AppData\Local\Temp\Eqtthwte	sqlite
		MD5: 46A7758AC3C84B687720253442F2EADE	**SHA256:** 71304D0BF373897D5A1942765036B52A8E4D4E52F707355E2F8188A3E0780FC0
3304	rundll32.exe	C:\Users\admin\AppData\Local\Temp\Fhfsey	binary
		MD5: F47EB60CDF981C17722D0CE740129927	**SHA256:** 0210071DF12CA42D70DCB679926668AE072264705AC139A24F94BBC5A129DD8F

6.- ¿Cuál es el hash MD5 del segundo archivo malicioso?

E758E07113016ACA55D9EDA2B0FFEEBE

3672	wscript.exe	C:\Users\admin\AppData\Local\Temp\JffleeTicl.dll	executable
		MD5: E758E07113016ACA55D9EDA2B0FFEEBE	**SHA256:** 2597322A49A6252445CA4C8D713320B238113B3B8FD8A2D6FC1088A5934CEE0E