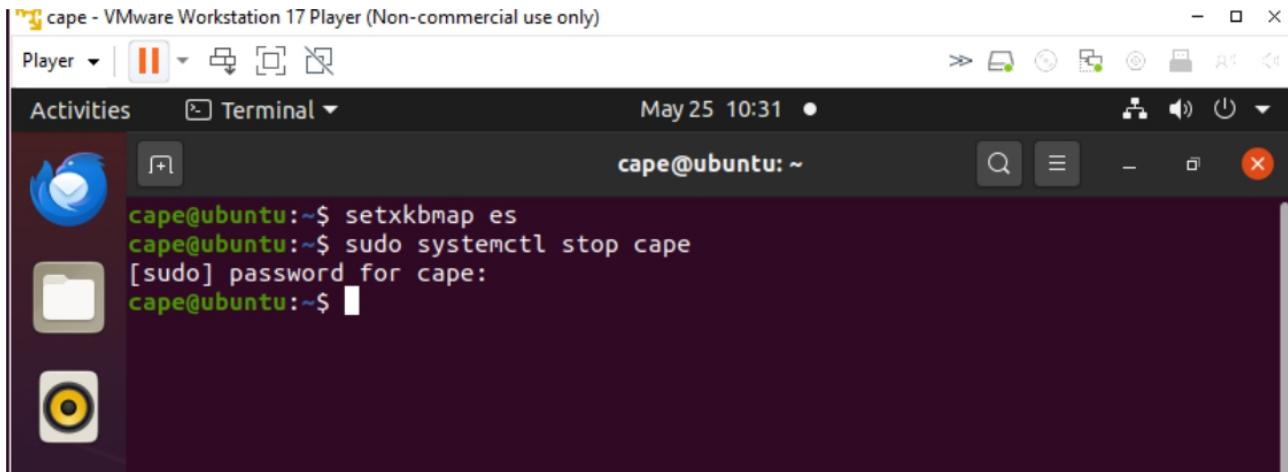


ANÁLISIS DE MALWARE

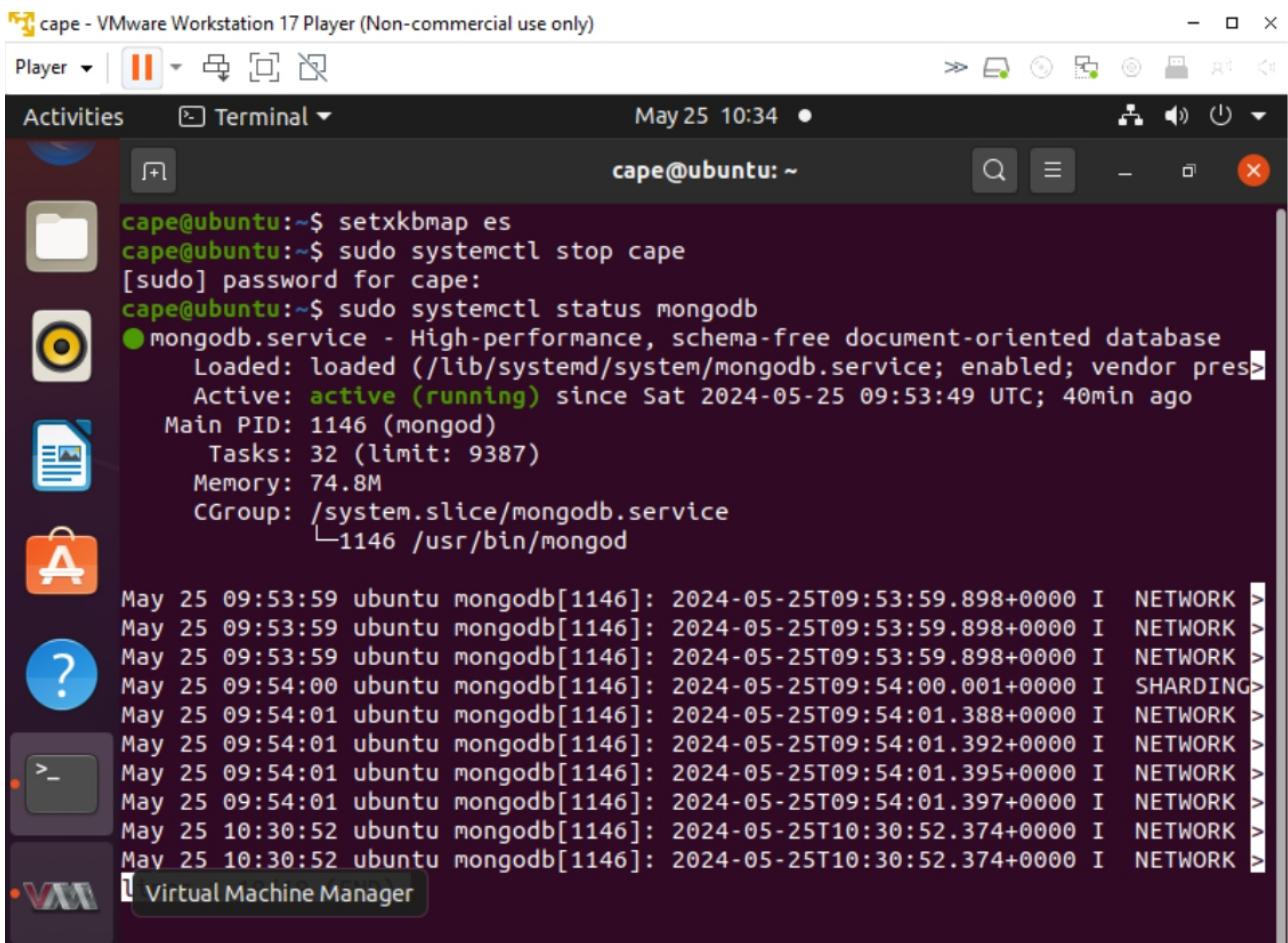
Primero realizo unas comprobaciones de que los servicios funcionan:

paro el servicio cape: sudo systemctl stop cape



```
cape@ubuntu:~$ setxkbmap es
cape@ubuntu:~$ sudo systemctl stop cape
[sudo] password for cape:
cape@ubuntu:~$
```

compruebo el estado de la bbdd mongodb: sudo systemctl status mongodb

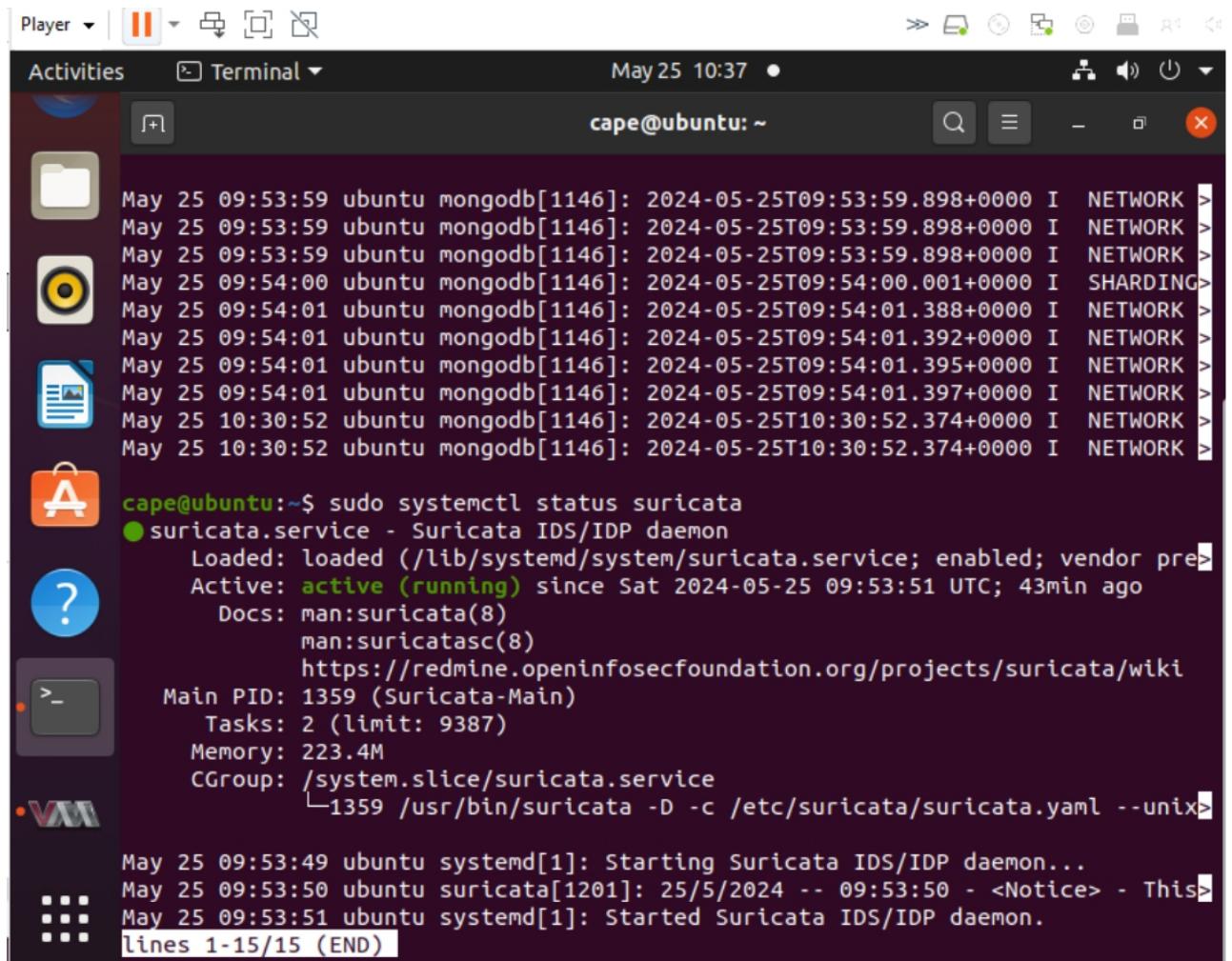


```
cape@ubuntu:~$ setxkbmap es
cape@ubuntu:~$ sudo systemctl stop cape
[sudo] password for cape:
cape@ubuntu:~$ sudo systemctl status mongodb
● mongodb.service - High-performance, schema-free document-oriented database
   Loaded: loaded (/lib/systemd/system/mongodb.service; enabled; vendor pres
     Active: active (running) since Sat 2024-05-25 09:53:49 UTC; 40min ago
       Main PID: 1146 (mongod)
          Tasks: 32 (limit: 9387)
         Memory: 74.8M
            CPU: 0.000 CPU(s) used
           CGroup: /system.slice/mongodb.service
                   └─1146 /usr/bin/mongod

May 25 09:53:59 ubuntu mongodb[1146]: 2024-05-25T09:53:59.898+0000 I NETWORK >
May 25 09:53:59 ubuntu mongodb[1146]: 2024-05-25T09:53:59.898+0000 I NETWORK >
May 25 09:53:59 ubuntu mongodb[1146]: 2024-05-25T09:53:59.898+0000 I NETWORK >
May 25 09:54:00 ubuntu mongodb[1146]: 2024-05-25T09:54:00.001+0000 I SHARDING>
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.388+0000 I NETWORK >
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.392+0000 I NETWORK >
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.395+0000 I NETWORK >
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.397+0000 I NETWORK >
May 25 10:30:52 ubuntu mongodb[1146]: 2024-05-25T10:30:52.374+0000 I NETWORK >
May 25 10:30:52 ubuntu mongodb[1146]: 2024-05-25T10:30:52.374+0000 I NETWORK >
```

el active está en verde, con lo cual activa la bbdd

compruebo el estado de suricata: sudo systemctl status suricata



The screenshot shows a terminal window on an Ubuntu desktop. The terminal title is "cape@ubuntu: ~". The window contains the following text:

```
May 25 09:53:59 ubuntu mongodb[1146]: 2024-05-25T09:53:59.898+0000 I NETWORK >
May 25 09:53:59 ubuntu mongodb[1146]: 2024-05-25T09:53:59.898+0000 I NETWORK >
May 25 09:53:59 ubuntu mongodb[1146]: 2024-05-25T09:53:59.898+0000 I NETWORK >
May 25 09:54:00 ubuntu mongodb[1146]: 2024-05-25T09:54:00.001+0000 I SHARDING>
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.388+0000 I NETWORK >
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.392+0000 I NETWORK >
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.395+0000 I NETWORK >
May 25 09:54:01 ubuntu mongodb[1146]: 2024-05-25T09:54:01.397+0000 I NETWORK >
May 25 10:30:52 ubuntu mongodb[1146]: 2024-05-25T10:30:52.374+0000 I NETWORK >
May 25 10:30:52 ubuntu mongodb[1146]: 2024-05-25T10:30:52.374+0000 I NETWORK >

cape@ubuntu:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor pre>
   Active: active (running) since Sat 2024-05-25 09:53:51 UTC; 43min ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://redmine.openinfosecfoundation.org/projects/suricata/wiki
   Main PID: 1359 (Suricata-Main)
     Tasks: 2 (limit: 9387)
    Memory: 223.4M
      CGroup: /system.slice/suricata.service
              └─1359 /usr/bin/suricata -D -c /etc/suricata/suricata.yaml --unix>

May 25 09:53:49 ubuntu systemd[1]: Starting Suricata IDS/IDP daemon...
May 25 09:53:50 ubuntu suricata[1201]: 25/5/2024 -- 09:53:50 - <Notice> - This>
May 25 09:53:51 ubuntu systemd[1]: Started Suricata IDS/IDP daemon.
lines 1-15/15 (END)
```

también está activa

luego sudo systemctl status suricata update.timer

```
cape@ubuntu:~$ sudo systemctl status suricata update.timer
Unit update.timer could not be found.

● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor pre>
   Active: active (running) since Sat 2024-05-25 09:53:50 UTC; 45min ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://redmine.openinfosecfoundation.org/projects/suricata/wiki
      Main PID: 1359 (Suricata-Main)
        Tasks: 2 (limit: 9387)
       Memory: 223.4M
      CGroup: /system.slice/suricata.service
              └─1359 /usr/bin/suricata -D -c /etc/suricata/suricata.yaml --unix>

May 25 09:53:49 ubuntu systemd[1]: Starting Suricata IDS/IDP daemon...
May 25 09:53:50 ubuntu suricata[1201]: 25/5/2024 -- 09:53:50 - <Notice> - This>
May 25 09:53:51 ubuntu systemd[1]: Started Suricata IDS/IDP daemon.

cape@ubuntu:~$ sudo systemctl status suricata update.timer
Unit update.timer could not be found.

● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor pre>
   Active: active (running) since Sat 2024-05-25 09:53:51 UTC; 45min ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://redmine.openinfosecfoundation.org/projects/suricata/wiki
      Main PID: 1359 (Suricata-Main)
        Tasks: 2 (limit: 9387)
       Memory: 221.6M
      CGroup: /system.slice/suricata.service
              └─1359 /usr/bin/suricata -D -c /etc/suricata/suricata.yaml --unix>

May 25 09:53:49 ubuntu systemd[1]: Starting Suricata IDS/IDP daemon...
May 25 09:53:50 ubuntu suricata[1201]: 25/5/2024 -- 09:53:50 - <Notice> - This>
May 25 09:53:51 ubuntu systemd[1]: Started Suricata IDS/IDP daemon.
lines 1-16/16 (END)
```

lanzo el script /tcpdump_user.sh

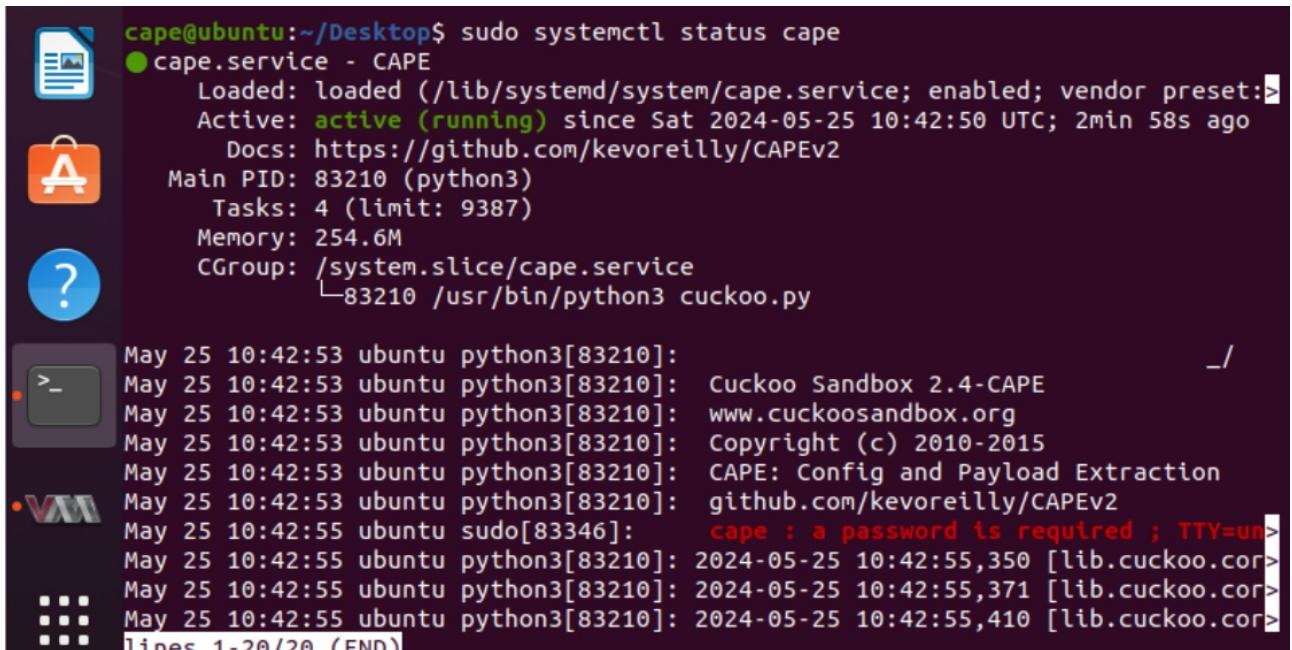
```
cape@ubuntu:~/Desktop/$ cd Desktop/
cape@ubuntu:~/Desktop$ ./tcpdump_user.sh
cape@ubuntu:~/Desktop$
```

compruebo el cape-rooter

```
cape@ubuntu:~/Desktop$ sudo systemctl status cape-rooter
● cape-rooter.service - CAPE rooter
   Loaded: loaded (/lib/systemd/system/cape-rooter.service; enabled; vendor pre>
   Active: active (running) since Sat 2024-05-25 09:53:49 UTC; 50min ago
     Docs: https://github.com/kevoreilly/CAPEv2
      Main PID: 1125 (python3)
        Tasks: 1 (limit: 9387)
       Memory: 7.7M
      CGroup: /system.slice/cape-rooter.service
              └─1125 /usr/bin/python3 rooter.py --iptables /usr/sbin/iptables ->

May 25 09:53:49 ubuntu systemd[1]: Started CAPE rooter.
lines 1-11/11 (END)
```

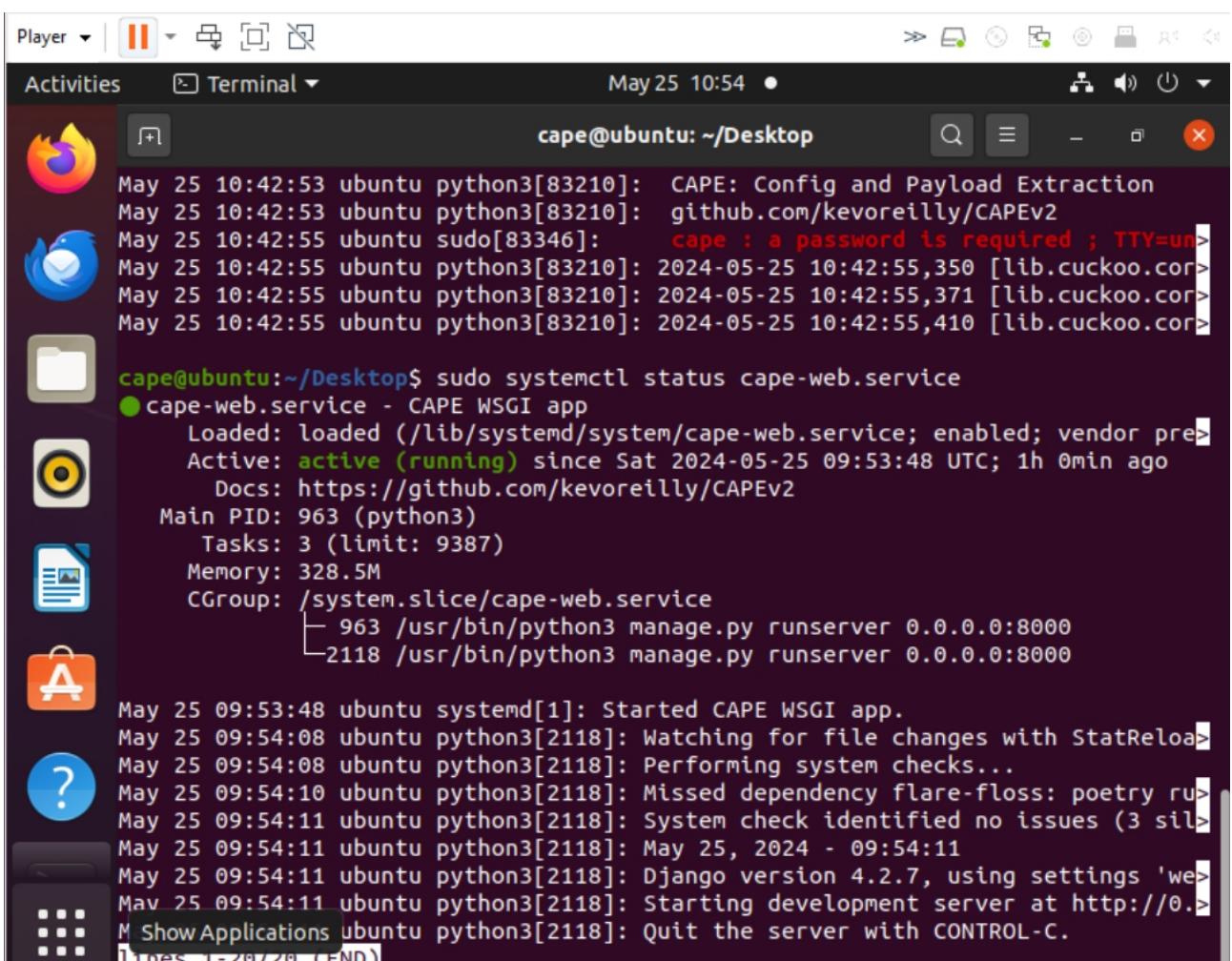
compruebo el cape normal



```
cape@ubuntu:~/Desktop$ sudo systemctl status cape
● cape.service - CAPE
   Loaded: loaded (/lib/systemd/system/cape.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-05-25 10:42:50 UTC; 2min 58s ago
     Docs: https://github.com/kevoreilly/CAPEv2
     Main PID: 83210 (python3)
        Tasks: 4 (limit: 9387)
       Memory: 254.6M
      CGroup: /system.slice/cape.service
              └─ 83210 /usr/bin/python3 cuckoo.py

May 25 10:42:53 ubuntu python3[83210]: CAPE: Config and Payload Extraction
May 25 10:42:53 ubuntu python3[83210]: github.com/kevoreilly/CAPEv2
May 25 10:42:53 ubuntu sudo[83346]:    cape : a password is required ; TTY=un
May 25 10:42:55 ubuntu python3[83210]: 2024-05-25 10:42:55,350 [lib.cuckoo.cor
May 25 10:42:55 ubuntu python3[83210]: 2024-05-25 10:42:55,371 [lib.cuckoo.cor
May 25 10:42:55 ubuntu python3[83210]: 2024-05-25 10:42:55,410 [lib.cuckoo.cor
lines 1-20/20 (END)
```

luego compruebo el cape web



```
Player | II | Activities Terminal May 25 10:54 ●
Activities Terminal May 25 10:54 ●
cape@ubuntu: ~/Desktop
May 25 10:42:53 ubuntu python3[83210]: CAPE: Config and Payload Extraction
May 25 10:42:53 ubuntu python3[83210]: github.com/kevoreilly/CAPEv2
May 25 10:42:55 ubuntu sudo[83346]:    cape : a password is required ; TTY=un
May 25 10:42:55 ubuntu python3[83210]: 2024-05-25 10:42:55,350 [lib.cuckoo.cor
May 25 10:42:55 ubuntu python3[83210]: 2024-05-25 10:42:55,371 [lib.cuckoo.cor
May 25 10:42:55 ubuntu python3[83210]: 2024-05-25 10:42:55,410 [lib.cuckoo.cor

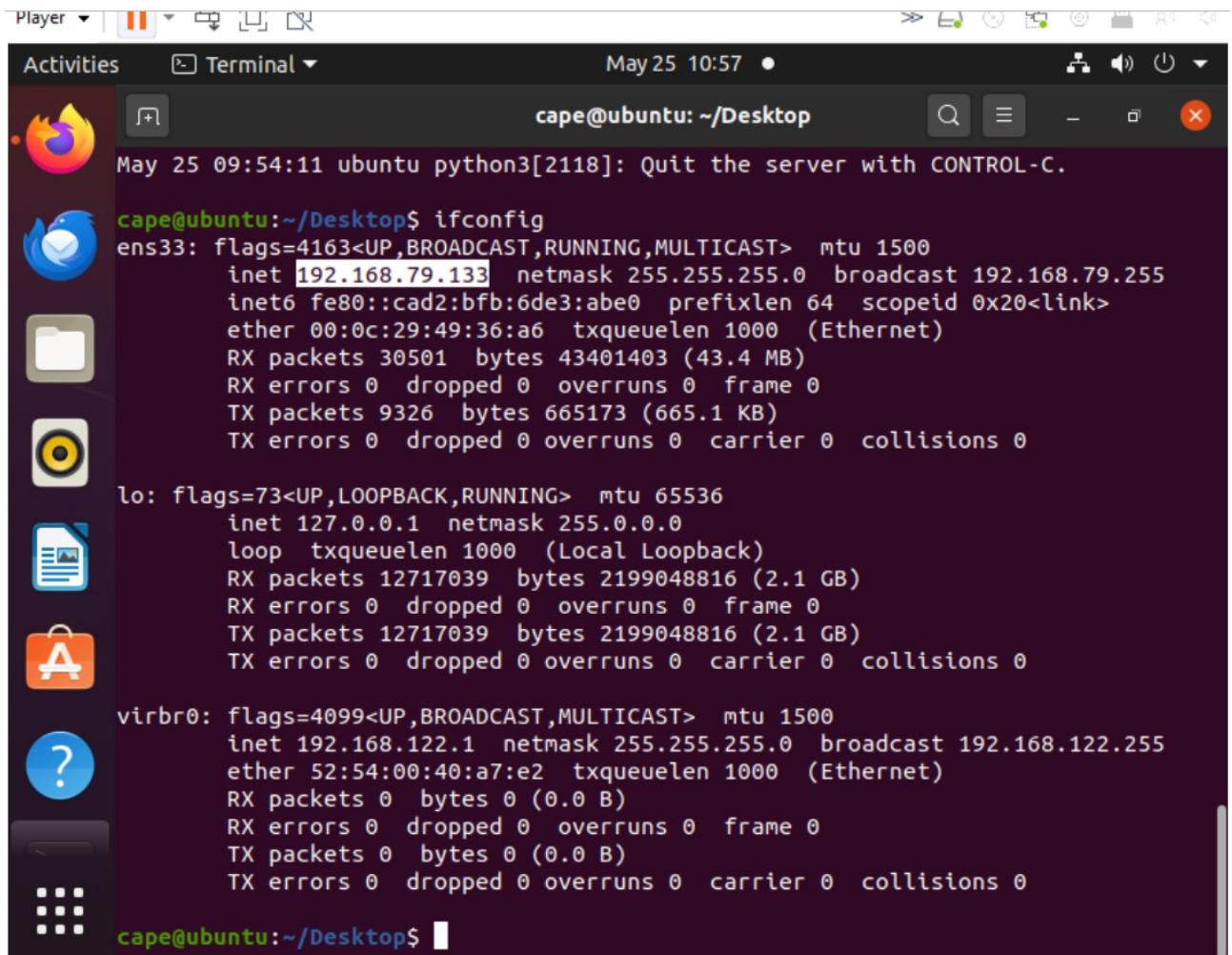
cape@ubuntu:~/Desktop$ sudo systemctl status cape-web.service
● cape-web.service - CAPE WSGI app
   Loaded: loaded (/lib/systemd/system/cape-web.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-05-25 09:53:48 UTC; 1h 0min ago
     Docs: https://github.com/kevoreilly/CAPEv2
     Main PID: 963 (python3)
        Tasks: 3 (limit: 9387)
       Memory: 328.5M
      CGroup: /system.slice/cape-web.service
              └─ 963 /usr/bin/python3 manage.py runserver 0.0.0.0:8000
                  ├─ 2118 /usr/bin/python3 manage.py runserver 0.0.0.0:8000

May 25 09:53:48 ubuntu systemd[1]: Started CAPE WSGI app.
May 25 09:54:08 ubuntu python3[2118]: Watching for file changes with StatReload...
May 25 09:54:08 ubuntu python3[2118]: Performing system checks...
May 25 09:54:10 ubuntu python3[2118]: Missed dependency flare-floss: poetry run
May 25 09:54:11 ubuntu python3[2118]: System check identified no issues (3 silen
May 25 09:54:11 ubuntu python3[2118]: May 25, 2024 - 09:54:11
May 25 09:54:11 ubuntu python3[2118]: Django version 4.2.7, using settings 'we
May 25 09:54:11 ubuntu python3[2118]: Starting development server at http://0.0.0.0:8000
May 25 09:54:11 ubuntu python3[2118]: Quit the server with CONTROL-C.
lines 1-20/20 (END)
```

con estas comprobaciones me aseguro que todo está listo para analizar malware

ahora voy a la web:

copio mi ip



The screenshot shows a standard Ubuntu desktop interface. On the left is a vertical dock with icons for various applications: Player, Activities, Terminal, Dash, Home, Computer, Help, and a question mark. The main area is a terminal window titled 'Terminal'. The terminal shows the command 'ifconfig' being run by the user 'cape@ubuntu'. The output displays network interface information for 'ens33', 'lo', and 'virbr0'. The IP address 192.168.79.133 is listed under the 'inet' entry for 'ens33'. The terminal prompt 'cape@ubuntu:' is visible at the bottom.

```
May 25 09:54:11 ubuntu python3[2118]: Quit the server with CONTROL-C.

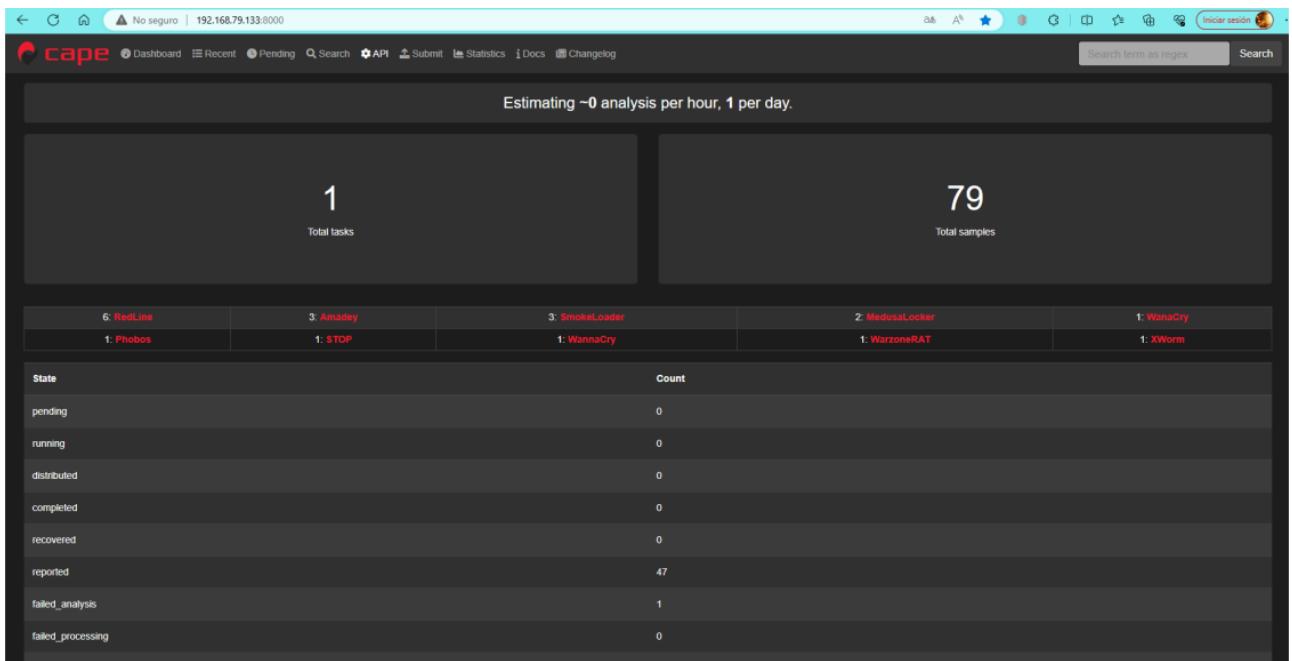
cape@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.79.133  netmask 255.255.255.0  broadcast 192.168.79.255
          inet6 fe80::cad2:bfb:6de3:abe0  prefixlen 64  scopeid 0x20<link>
            ether 00:0c:29:49:36:a6  txqueuelen 1000  (Ethernet)
              RX packets 30501  bytes 43401403 (43.4 MB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 9326  bytes 665173 (665.1 KB)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      loop  txqueuelen 1000  (Local Loopback)
        RX packets 12717039  bytes 2199048816 (2.1 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12717039  bytes 2199048816 (2.1 GB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
      inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
            ether 52:54:00:40:a7:e2  txqueuelen 1000  (Ethernet)
              RX packets 0  bytes 0 (0.0 B)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 0  bytes 0 (0.0 B)
              TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

cape@ubuntu:~/Desktop$
```

me voy al navegador de mi equipo anfitrión a la esa ip con puerto 8000



aquí tengo la interface de Cape con la que voy a analizar malware
pincho en Recent y en el 73, que es la muestra que voy a analizar:

esta es la pantalla de la muestra 73

Datos de la muestra:

-PE32 (es un ejecutable)
 -MD5 ffc5e9ebe857d45fa5f578593342ede53
 - SHA1 6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c
 -SHA256 82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19

Este no tiene packer, con lo cual es probable que no tenga payload
aquí tengo la interface de Cape con la que voy a analizar malware
pincho en Recent y en el 73, que es la muestra que voy a analizar:

ID	Timestamp	Machine	Package	Filename	MD5	Detections	Task tags	PK /HTTP/TLS/F	Files	VT	MalScore	PCA	P	ClamAV	Status
80	2023-12-02 00:18:14	win7	exe	3928.exe	e8e783bba2f8e3fd2da2bded27eceed	SmokeLoader	false	exe 0/-/-/-	-	10.0	PCAP	-			reported
79	2023-12-02 00:12:37	win7	exe	B65B.exe	33a60439e95f0dfc10016075f97ae8b0c	SmokeLoader	false	exe 0/-/-/-	-	10.0	PCAP	-			reported
78	2023-12-01 23:44:16	win7	exe	quasarRAT.bat.exe	92f44e405db16ac55d97e3bf3b132fa		false	exe 0/-/-/-	-	2.0	PCAP	-			reported
77	2023-12-01 23:12:56	win7	exe	XClient.exe	e47a5d191f8acb69797887ab43b24370	XWorm		exe 0/-/-/-	-	1.0	PCAP	-			reported
76	2023-12-01 23:28:23	win7	generic	quasarRAT.bat	09a47e33c5bcc69e9fd6a34bb966197d			gpn 0/-/-/-	-	0.0	PCAP	-			reported
75	2023-12-01 22:51:43	win7	exe	e5372acb7610fb1bed6.exe	887e0e9454a36659cd7a08dd94425c1e			exe 0/-/-/-	-	1.0	PCAP	-			reported
74	2023-12-01 16:17:02	win7	exe	1100b4580e629445e005c2	54ecd7b2d5a1a4e14160c7812efa1237			exe 0/-/-/-	-	2.0	PCAP	-			reported
73	2023-12-01 18:09:47	win7	exe	82d763b6cd97ca240a29.exe	fc5e9ebe857d45fa5f578593342ede53	SmokeLoader		exe 464/-/-/-	-	10.0	PCAP	-			reported
72	2023-12-01 17:45:13	win7	exe	1100b4580e6299445e00.exe	54ecd7b2d5a1a4e14160c7812efa1237			exe 0/-/-/-	-	2.0	PCAP	-			reported
71	2023-12-01 17:17:48	win7	lnk	forelouper.lnk	c49299cd970aa9c6a1938e59033bd3b8		false	lnk 0/-/-/-	-	2.0	PCAP	-			reported

esta es la pantalla de la muestra 73

Analysis

Category	Package	Started	Completed	Duration	Options	Log(s)	MalScore
FILE	exe	2023-12-01 17:45:13	2023-12-01 18:09:47	1474 seconds	Show Options	Show Analysis Log	10.0

Machine

Name	Label	Manager	Started On	Shutdown On	Route
win7	win7	KVM	2023-12-01 17:45:13	2023-12-01 18:09:46	internet

SmokeLoader Config

Type	SmokeLoader Config
C2s	* http://go-piratia.ru/tmp/index.php * http://humydrole.com/tmp/index.php * http://pirateking.online/tmp/index.php * http://piratia.pw/tmp/index.php * http://piratia.ru/tmp/index.php
Extracted From	sha256: e71538aa78cc661ff94e8a9ee72cd3c9da934dcc4ecf6a5d8aef1ff16ce2b2e sha256: 3002b01c9a8acd8301a29e8e36ba988dad933c0128e1ebd430de9559fb2d272 sha256: ede5038dbde934e28afdb273cea8e655dbd7ea0588baed4a9b478cd03cd245

File Details

File Name	82d763b6cd97ca240a29.exe
File Type	PE32 executable (GUI) Intel 80386, for MS Windows

Datos de la muestra:

-PE32 (es un ejecutable)

-MD5 ffc5e9ebe857d45fa5f578593342ede53 - SHA1 6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c
-SHA256 82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19 Este no tiene packer, con lo cual es probable que no tenga payload

Strings:

An application has made an attempt to load the C runtime library incorrectly. Dice que una aplicación ha intentado cargar incorrectamente una librería C

DeleteCriticalSection borra una sección crítica

This indicates a bug in your application. It is most likely the result of calling an MSIL-compiled (/clr) function from a native constructor or from DllMain. Informa de un bug en la aplicación

`SetConsoleCursorPosition` establece la posición del cursor

Copyright (C) 2022, Crazy deja el copyright

`USER32.DLL` carga una dll, es un enlace para hacer llamadas al kernel de microsoft

`WriteFile` escribe en un fichero

This application has requested the Runtime to terminate it in an unusual way. Esta aplicación ha pedido la ejecución para terminar de forma no usual

- Attempt to initialize the CRT more than once. Intento de inicializar el CRT más de una vez

`Microsoft Visual C++ Runtime Library` carga una librería visual c++

- Attempt to use MSIL code from this assembly during native code initialization. Intento de usar un código MSIL desde el código ensamblador durante la inicialización del código nativo

`GetProcessWindowStation` intenta conseguir el proceso de una ventana

veo que me da un MalScore de 10.0 que es el parámetro de peligrosidad, es decir, muy peligroso

datos de la máquina virtual donde se ha analizado:

Machine						PE Information			Sections								
Name	Label	Manager	Started On	Shutdown On	Route	Image Base	Entry Point	Reported Checksum	Actual Checksum	Minimum OS Version	PDB Path	Compile Time	Import Hash	Icon	Icon Exact Hash	Icon Similarity Hash	Icon DHash
win7	win7	KVM	2023-12-01 17:45:13	2023-12-01 18:09:46	internet	0x00040000	0x0000	0x00054a66	0x00054a66	5.0	C:\slir64_nyexofavubix-puzadidzopoga25-wowunugibuhern78ib.pdb	2022-12-05 15:35:42	1756ec87e9180426f96d9ce779d24407		24a118ed3241d13d070bf74a4479cc	31b3e7b0995cc97ed9db65975ab3069	40d8dac262aaa2b0

en la sección de PE Information no viene nada interesante, viene el copyright el nombre original del fichero y las versiones

PE Information											
FileDescription	Malling										
LegalCopyright	Copyright (C) 2022, Crazy										
OriginalFilename	Mangler										
ProductsVersion	19.3.71.61										
ProductionVersion	16.78.79.2										
Translation	0x25ad 0x0be92										

en la sección Sections

Sections						
Name	RAW Address	Virtual Address	Virtual Size	Size of Raw Data	Characteristics	Entropy
.text	0x0000400	0x00001000	0x00028f56	0x00029000	IMAGE_SCN_CNT_CODE IMAGE_SCN_MEM_EXECUTE IMAGE_SCN_MEM_READ	6.84
.data	0x00029400	0x0002a000	0x0267557c	0x00001800	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ IMAGE_SCN_MEM_WRITE	2.84
.rsrc	0x0002ac00	0x026a0000	0x000208f0	0x00020a00	IMAGE_SCN_CNT_INITIALIZED_DATA IMAGE_SCN_MEM_READ	4.22

tienen entropía baja < 7,5 con lo cual no hay datos cifrados, no hay payload

Imports:

Kernel32: gestión ficheros, localiza en memoria las direcciones

User32: imprime mensaje

ADVAPI32: posible cifrado

aquí tengo los datos del fichero, como los hashes:

File Details	
File Name	82d763b6cd97ca240a29.exe
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
File Size	308736 bytes
MD5	fc5e9eb857d45fa5578593342ede53
SHA1	6604057c56d1ef3e30c4563d0a8ab41bf9fea5c
SHA256	82d763b6cd97ca240a291c90b6de517232b92cbbe5b693549a61547a30ecbf19 [V] [MWDB] [Bazaar]
SHA3-384	30a9a95df5dcf6c2ad741b0aef50ff575de999db338d6e9e640583cf2606f518734b52562ea050542b94fe159660b
CRC32	296CEADF
TLSH	T15164F85382F1BD44E9268B729F2FE6EC775DF6508F8A776922189E1F40B1172C263B10
Ssdeep	3072.Fi+D6UfsY7Oy4kzCEuCBlyj55ulg9vcYS15GzGhzLUX558.56Ufx7Oy42BojClsa22A
PE	

PE Information											
Image Base	Entry Point	Reported Checksum	Actual Checksum	Minimum OS Version	PDB Path	Compile Time	Import Hash	Icon	Icon Exact Hash	Icon Similarity Hash	Icon DHash
0x0040 0000	0x0000 3749	0x00054a86	0x00054a86	5.0	C:\src64_nyexofavubtx-puzadidzopogzis-wowurugibuhen78ib.pdb	2022-12-05 15:35:42	1756ec87e9180426969ce77 9d24407		24a118ed3241d13d07f0bf74a 4479cc	31b3e7b0995cc97ed9db659f7 5ab3b69	40d9dac2b2aaa2b0
Version Infos											
FileVersion	1.0.0.0	FileDescription	Malling	ProductVersion	1.0.0.0	LegalCopyright	Copyright (C) 2022, Crazy	OriginalFilename	Mumper	ProductionVersion	1.0.0.0
Translation	0x25ed 0x0e92	FileDescription	Malling	ProductVersion	1.0.0.0	LegalCopyright	Copyright (C) 2022, Crazy	OriginalFilename	Mumper	ProductionVersion	1.0.0.0

pincho en Mitre, que son los comportamientos que ha detectado del malware:

Mitre ATT&CK								
Discovery	Credential Access	Execution	Collection	Persistence	Privilege Escalation	Defense Evasion	Command and Control	Impact
• T1033 - System Owner/User Discovery <ul style="list-style-type: none"> ◦ encrypt_pcinfo 	• T1003 - OS Credential Dumping <ul style="list-style-type: none"> ◦ infostealer_mail ◦ infostealer_browser 	• T1129 - Shared Modules <ul style="list-style-type: none"> ◦ dropper 	• T1114 - Email Collection <ul style="list-style-type: none"> ◦ infostealer_mail 	• T1547 - Boot or Logon Autostart Execution <ul style="list-style-type: none"> ◦ persistence_autorun 	• T1547 - Boot or Logon Autostart Execution <ul style="list-style-type: none"> ◦ persistence_autorun 	• T1564 - Hide Artifacts <ul style="list-style-type: none"> ◦ stealth_window 	• T1071 - Application Layer Protocol <ul style="list-style-type: none"> ◦ injection_network_traffic 	• T1486 - Data Encrypted for Impact <ul style="list-style-type: none"> ◦ ransomware_file_modifications
• T1082 - System Information Discovery <ul style="list-style-type: none"> ◦ antivm_generic_diskskreg ◦ recon_fingerprint ◦ antivm_generic_bios ◦ antivm_generic_system 	• T1539 - Steal Web Session Cookie <ul style="list-style-type: none"> ◦ infostealer_cookie 	• T1106 - Native API process_creation_suspicious_localization <ul style="list-style-type: none"> ◦ antidebug_guardpages 	• T1005 - Data from Local System <ul style="list-style-type: none"> ◦ infostealer_mail ◦ infostealer_browser 	• T1547.001 - Registry Run Keys / Startup Folder <ul style="list-style-type: none"> ◦ persistence_autorun 	• T1055 - Process Injection <ul style="list-style-type: none"> ◦ injection_inter_process ◦ explorer_http 	• T1202 - Indirect Command Execution <ul style="list-style-type: none"> ◦ suspicious_commands_and_tools ◦ uses_windows_utils_files 	• network_multiple_direct_ip_connections <ul style="list-style-type: none"> ◦ suspicious_tld ◦ explorer_http ◦ network_cnc_http ◦ network_smtp ◦ suricata_alert ◦ powershell_request 	• T1485 - Data Destruction <ul style="list-style-type: none"> ◦ anomalous_delete_file
• T1010 - Application Window Discovery <ul style="list-style-type: none"> ◦ antidebug_windows 	• T1555 - Credentials from Password Stores <ul style="list-style-type: none"> ◦ infostealer_browser 	• T1059.001 - PowerShell <ul style="list-style-type: none"> ◦ powershell_downloads ◦ powershell_requests 	• T1560 - Archive Collected Data <ul style="list-style-type: none"> ◦ encrypt_pcinfo 		• T1547.001 - Registry Run Keys / Startup Folder <ul style="list-style-type: none"> ◦ persistence_autorun 	• T1562 - Impair Defenses <ul style="list-style-type: none"> ◦ antisandbox_uhoh_0ok 	• T1036 - Masquerading <ul style="list-style-type: none"> ◦ explorer_http 	
• T1083 - File and Directory Discovery <ul style="list-style-type: none"> ◦ antemu_winefend 	• T1555.003 - Credentials from Web Browsers <ul style="list-style-type: none"> ◦ infostealer_browser 				• T1055 - Process Injection <ul style="list-style-type: none"> ◦ injection_inter_process ◦ explorer_http 	• T1090 - Proxy <ul style="list-style-type: none"> ◦ network_tor 	• T1090.003 - Multi-hop Proxy <ul style="list-style-type: none"> ◦ network_tor 	
• T1497 - Virtualization/Sandbox Evasion <ul style="list-style-type: none"> ◦ antivm_generic_diskskreg ◦ antivm_generic_system ◦ antivm_generic_bios ◦ antivm_vbox_keys ◦ antemu_winefend 	• T1552 - Credentials in Files <ul style="list-style-type: none"> ◦ infostealer_mail ◦ infostealer_browser 				• T1112 - Modify Registry <ul style="list-style-type: none"> ◦ persistence_autorun ◦ powershell_downloads 	• T1090.003 - Multi-hop Proxy <ul style="list-style-type: none"> ◦ network_tor 	• T1573 - Encrypted Channel <ul style="list-style-type: none"> ◦ network_cnc_https_tempstorage ◦ network_cnc_https 	
• T1057 - Process					• T1070 - Indicator Removal			

Discovery: Obtención usuarios del sistema

Credencial access: intenta robar credenciales cookies de los navegadores

Execution: módulos compartidos de la API de Microsoft, rutas compartidas, carpetas de red, crea un proceso sospechoso, ejecutar órdenes al sistema con PowerShell.

Collection: roba información de emails, datos del sistema local

Persistencia: crea persistencia al inicio del sistema, a través de claves de registro o de inicio.

Privilege Escalation: ejecución como system. Escalado de privilegios, como administrador.

Defense evasion: esconde ficheros en ruta, o los ejecuta en segundo plano, ejecución indirecta de comandos, modifica registro para persistencia, borra historial de navegación.

Command and control: conexiones sospechosas de red mirar Suricata, hay un proxy que se conecta a Tor. Cifra canales

Impact: es un ramsonware modifica datos, y destruye datos.

Conclusión: estamos ante un Ramsonware que cifra, hace conexiones sospechosas de red a la botnet a través de Tor, roba información de correos, escala privilegios, esconde ficheros o los ejecuta en segundo plano. Con la herramienta PowerShell.

Signatures:

Signatures
Collects and encrypts information about the computer likely to send to C2 server
SetUnhandledExceptionFilter detected (possible anti-debug)
Checks adapter addresses which can be used to detect virtual network interfaces
At least one process apparently crashed during execution
Possible date expiration check, exits too soon after checking local time
Uses Windows utilities for basic functionality

Colecciona y encripta información del sistema local a través de una botnet

Se ha detectado un **SetUnhandledExceptionFilter** posible antidebug

Se ha detectado un **GetAdaptersAddresses** le sirve al malware para comprobar que esté en una maquina virtual

Lanza unos comandos crea carpetas, copia los ficheros infectados, y hace ping a localhost

Método anti-sandbox: comprueba la hora local de cuando se creó la máquina. Comprueba antigüedad de máquina.

Anomalous file deletion behavior detected (10+)
Guard pages use detected - possible anti-debugging
A process attempted to delay the analysis task
Attempts to connect to a dead IP:Port (892 unique times)
Dynamic (imported) function loading detected
Performs HTTP requests potentially not found in PCAP
HTTPS urls from behavior
Establishes an encrypted HTTPS connection
Data downloaded by powershell script
Powershell is sending data to a remote host
Enumerates the modules from a process (may be used to locate base addresses in process injection)
Enumerates running processes
Expresses interest in specific running processes
Repeatedly searches for a not-found process, may want to run with startbrowser=1 option
Reads data out of its own binary image
A process created a hidden window
Terminates another process
NtSetInformationThread: attempt to hide thread from debugger
CAPE extracted potentially suspicious content
Drops a binary and executes it
Creates RWX memory

Se detectan anomalías

Se detecta que intenta conectarse a una serie de ips

Attempts to connect to a dead IP:Port (892 unique times)
IP: 35.186.223.180:2222 (unknown)
IP: 104.47.13.36:995 (unknown)
IP: 47.246.137.47:995 (unknown)
IP: 52.101.8.32:587 (unknown)
IP: 86.35.15.70:443 (unknown)
IP: 20.74.67.225:995 (unknown)
IP: 104.47.1.36:220 (unknown)
IP: 3.64.119.87:990 (unknown)
IP: 52.101.11.7:465 (unknown)
IP: 86.35.15.70:110 (unknown)
IP: 3.33.130.190:80 (unknown)
IP: 52.101.73.16:587 (unknown)
IP: 172.65.182.103:25 (unknown)
IP: 104.26.14.11:2222 (unknown)
IP: 104.47.17.138:2525 (unknown)
IP: 162.159.135.42:222 (unknown)
IP: 185.183.194.90:443 (unknown)
IP: 31.25.12.19:22 (unknown)
IP: 52.71.130.112:21 (unknown)

Se detecta que ejecuta algunas funciones:

Dynamic (imported) function loading detected
DynamicLoader: ntdll.dll/RtlExitUserThread
DynamicLoader: IMM32.dll/ImmIsIME
DynamicLoader: IMM32.dll/ImmGetContext
DynamicLoader: IMM32.dll/ImmLockMC
DynamicLoader: IMM32.dll/ImmUnlockMC
DynamicLoader: IMM32.dll/ImmReleaseContext
DynamicLoader: IMM32.dll/ImmSetCompositionFontW
DynamicLoader: IMM32.dll/ImmGetCompositionWindow
DynamicLoader: IMM32.dll/ImmSetCompositionWindow
DynamicLoader: CRYPTSP.dll/CryptHashData
DynamicLoader: CRYPTSP.dll/CryptGetHashParam
DynamicLoader: CRYPTSP.dll/CryptDestroyHash
DynamicLoader: CRYPTSP.dll/CryptReleaseContext
DynamicLoader: SSPICL.DLL/GetUserNameExW
DynamicLoader: ADVAPI32.dll/LookupAccountNameW
DynamicLoader: XmlLite.dll/CreateXmlWriter
DynamicLoader: XmlLite.dll/CreateXmlWriterOutputWithEncodingName
DynamicLoader: ole32.dll/CoInitializeEx
DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
DynamicLoader: ole32.dll/CoTaskMemAlloc
DynamicLoader: ole32.dll/StringFromID
DynamicLoader: NSI.dll/NsAllocateAndGetTable
DynamicLoader: CFGMGR32.dll/CM_Open_Class_Key_ExW
DynamicLoader: IPHLPAPI.DLL/ConvertInterfaceGuidToLuid
DynamicLoader: IPHLPAPI.DLL/GetEntry2
DynamicLoader: IPHLPAPI.DLL/GetForwardTable2
DynamicLoader: IPHLPAPI.DLL/GetNetEntry2
DynamicLoader: IPHLPAPI.DLL/FreeMmTable
DynamicLoader: ole32.dll/CoTaskMemFree
DynamicLoader: NSI.dll/NsFreeTable
DynamicLoader: ole32.dll/CoInitialize
DynamicLoader: SHLWAPI.dll/StrCmpNW
DynamicLoader: WS2_32.dll/GetAddInfoV
DynamicLoader: ADVAPI32.dll/RegDeleteTreeA
DynamicLoader: ADVAPI32.dll/RegDeleteTreeW
DynamicLoader: WS2_32.dll/WSASocketW

Enumera procesos

Enumerates running processes	
process:	System with pid 4
process:	sms.exe with pid 264
process:	cssss.exe with pid 352
process:	winninit.exe with pid 388
process:	cssss.exe with pid 400
process:	windlgon.exe with pid 436
process:	services.exe with pid 484
process:	lsass.exe with pid 492
process:	lsm.exe with pid 500
process:	svchost.exe with pid 592
process:	svchost.exe with pid 656
process:	svchost.exe with pid 760
process:	svchost.exe with pid 824
process:	svchost.exe with pid 848
process:	svchost.exe with pid 976
process:	svchost.exe with pid 112
process:	spoolsv.exe with pid 1012
process:	svchost.exe with pid 1116
process:	amsvc.exe with pid 1268
process:	svchost.exe with pid 1296
process:	svchost.exe with pid 1712
process:	taskhost.exe with pid 1896
process:	dwm.exe with pid 1964
process:	explorer.exe with pid 1988
process:	OSPPSVC.EXE with pid 620

Lee datos de su propio binario

Reads data out of its own binary image	
self_read: process: Perceived.pif, pid: 4668, offset: 0x3030785c3030785c, length: 0x00105860	

Crea un proceso en segundo plano

A process created a hidden window							
Time	TID	Caller	API	Arguments	Status	Return	Repeated
2023-12-01 15:42:18,906	353 2	0x723f737c 0x060a0257	CreateProcessInternalW	ApplicationName: C:\Users\ama\AppData\Local\Temp\288D.exe CommandLine: C:\Users\ama\AppData\Local\Temp\288D.exe CreationFlags: CREATE_SUSPENDED CREATE_NO_WINDOW ProcessId: 3432 ThreadId: 3440 ProcessHandle: 0x000000108 ThreadHandle: 0x000000104 StackPivoted: no	SUCCESS	0x00000001	3 times

Se ha detectado contenido potencialmente sospechoso

CAPE extracted potentially suspicious content	
288D_exe:	UPX
explorer_exe:	SmokeLoader
explorer_exe:	SmokeLoader
explorer_exe:	SmokeLoader
288D_exe:	UPX

Se detectan estos payloads:

binary: C:\Users\ama\AppData\Local\Temp\3928.exe
binary: C:\Users\ama\AppData\Local\Temp\B65B.exe

Comprueba la presencia de herramientas de depuración y forense

Checks for the presence of known windows from debuggers and forensic tools

```

Window_OLLYDBG
Window_GBDYLL0
Window_pedi06
Window_FilemonClass
Window_File Monitor - Sysinternals: www.sysinternals.com
Window_PROMON_WINDOW_CLASS
Window_Process Monitor - Sysinternals: www.sysinternals.com
Window_RegmonClass
Window_Registry Monitor - Sysinternals: www.sysinternals.com
Window_18467-41

```

Checks for the presence of known windows from debuggers and forensic tools

```

window_OLLYDBG
window_GBDYLL0
window_pedi06
window_FilemonClass
window_File Monitor - Sysinternals: www.sysinternals.com
window_PROMON_WINDOW_CLASS
window_Process Monitor - Sysinternals: www.sysinternals.com
window_RegmonClass
window_Registry Monitor - Sysinternals: www.sysinternals.com
window_18467-41

```

```

    " registryValue": "value\\regsvr32.exe \\v\\user\\temp\\942B.dll"
      * regsvr32.exe 2804 /s C:\\Users\\ama\\AppData\\Local\\Temp\\942B.dll
    o A89f.exe 3712
      * AppLaunch.exe 3026
        * WerFault.exe 3096 -u -p 3028 -s 624
    o B65B.exe 3512
    o explorer.exe 1936
    o explorer.exe 3944
    o B7C1.exe 2648
      * cmd.exe 5364 cmd/k cmd < Enjoyed & exit
        * cmd.exe 3516 cmd
          * tasklist.exe 8164 tasklist
          * findstr.exe 6589 findstr /R "avast! exe avgul.exe nswscsvc.exe sophoshealth.exe"
          * tasklist.exe 7752 tasklist
          * findstr.exe 6384 findstr /R "wsa.exe"
        * cmd.exe 4984 cmd/c midir 29768
        * cmd.exe 4732 cmd/c copy /b Infected + Tin + Exalted + Condo 29768\Perceived.pdf
        * cmd.exe 6048 cmd/c copy /b Orders + Cylinder 29768\Perceived.pdf 29768q
        * Perceived.pdf 4568 29768\Perceived.pdf 29768q
        * PING.EXE 6328 ping -n 5 localhost
    o explorer.exe 6980
    o explorer.exe 8136
    o explorer.exe 2220
    o explorer.exe 7040
    o explorer.exe 7048
    o explorer.exe 6096
    o explorer.exe 2268
    o explorer.exe 5724
    o explorer.exe 2140
    o ACF7.exe 2256
  * services.exe 484
    o svchost.exe 848 -k netsvc

```

Inicia sockets de escucha en estos puertos:

Starts servers listening on 127.0.0.1:23075, 127.0.0.1:0							
Time	TID	Caller	API	Arguments	Status	Return	Repeated
2023-12-01 15:43:48,389	398 0	0x71eb95e5 0x71eb8d02	bind	socket: 552 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:42:02,906	195 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 1304 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:42:03,797	269 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 1316 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:42:05,562	195 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 1332 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:42:07,156	269 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 1316 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:42:08,672	195 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 3252 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:42:16,234	269 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 3540 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times
2023-12-01 15:43:17,859	269 2	0x7efafa10086c 0x7efafa0f90ec	bind	socket: 3196 ip: 0.0.0.0 port: 0	SUCCESS	0x00000000	2 times

Detecta el antivirus Defender, Avast y Sandbox

Intenta eliminar evidencias

Attempts to remove evidence of file being downloaded from the Internet							
Time	TID	Caller	API	Arguments	Status	Return	Repeated
2023-12-01 15:41:56,109	327 2	0x0270216f 0x0a1012f0	DeleteFileW	FileName: C:\\Users\\ama\\AppData\\Roaming\\ribegga:zone.Identifier	failed	0x00000000	2 times

Se ha detectado este malware:

CAPE detected the SmokeLoader malware
 SmokeLoader. [{"Yara": "e7153aa78cc661ff94e8a9ee72c6d3c9da934dc4ecf5a5d8ae1fb16ce2b2e"}, {"Yara": "3002b01c9aacbd8301a29e8e136ba88adad833c0128e1ebd43dd8659f9d2272"}, {"Yara": "e0e5038dbde934e28fadb273cea8e655dbd7ear80588baed4a9b478cd03cd245"}]

Pincho en Behavioral Analysis para observar el análisis de comportamiento del malware:

The screenshot shows the CAPE Behavioral Analysis interface with the 'Process Tree' tab selected. The tree structure starts with the main process, 82d763b6cd97ca240a29.exe (PID: 772), which is identified as 'SmokeLoader'. It branches down through various system processes like explorer.exe, cmd.exe, and svchost.exe, along with several custom executables such as WerFault.exe, ACF7.exe, and taskhost.exe. Some of these custom executables have descriptive names like 'Perceived.pdf' or 'PING.EXE'. The tree also includes network-related processes like regsvr32.exe and file handlers like findstr.exe.

solo he encontrado dos ejecutables pero no sospechosos de ser malware.

Aquí veo las órdenes que ha lanzado al sistema windows:

The screenshot shows the CAPE Network Analysis interface with a list of API calls. The table has columns for Time, TID, Caller, API, Arguments, Status, Return, and Repeated. The API calls listed include NtDelayExecution, NtQueryValueKey, GetSystemTimeAsFileTime, HeapCreate, LdrGetDllHandle, and LdrGetProcAddress. Most calls are successful (Status: SUCCESS) and result in 0x00000000. There are a few failed calls (Status: failed) with invalid handles. The 'Repeated' column indicates that some calls were made multiple times, such as the NtDelayExecution call which was repeated 21 times.

Time	TID	Caller	API	Arguments	Status	Return	Repeated
2023-12-01 15:41:31.749	908	0x778bc7be 0x77899e59	NtDelayExecution	Milliseconds: 30 Status: Skipped	SUCCESS	0x00000000	21 times
2023-12-01 15:41:31.749	908	0x778bc7be 0x77899e59	NtDelayExecution	Status: skipped log limit reached	SUCCESS	0x00000000	2 times
2023-12-01 15:41:31.874	103	0x778c3046 0x778e13d2	NtQueryValueKey	KeyHandle: 0x00000000 ValueName: DisableUserModeCallbackFilter FullName: DisableUserModeCallbackFilter	failed	INVALID_HANDLE	2 times
2023-12-01 15:41:32.108	103	0x004060ec 0x0040374e	GetSystemTimeAsFileTime		SUCCESS	0x00000000	2 times
2023-12-01 15:41:32.108	103	0x0040609a 0x0040363e	HeapCreate	Options: 0 InitialSize: 0x00001000 MaximumSize: 0x00000000	SUCCESS	0x06a00000	2 times
2023-12-01 15:41:32.108	103	0x00404d1d 0x00000000	LdrGetDllHandle	FileName: KERNEL32.DLL ModuleHandle: 0x75d20000	SUCCESS	0x00000000	2 times
2023-12-01 15:41:32.108	103	0x00404d40 0x00000000	LdrGetProcAddress	ModuleName: kernel32.dll ModuleHandle: 0x75d20000 FunctionName: #1sAlloc Ordinal: 0 FunctionAddress: 0x75d34f2b	SUCCESS	0x00000000	2 times

pincho en Network Analysis, nos muestra un análisis de red:

cape

Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex Search

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

PCAP PCAP

Hosts (846) DNS (3724) TCP (10852) UDP (5093) HTTP (3082) SMTP (0) IRC (0) ICMP (218) Suricata Alerts (464) Suricata TLS (0) Suricata HTTP (0) Suricata Files (0)

Direct	IP	Country Name
N	185.164.14.7 [VT]	unknown
N	191.252.4.30 [VT]	unknown
N	34.251.138.12 [VT]	unknown
N	200.11.241.137 [VT]	unknown
N	15.161.213.100 [VT]	unknown
N	34.253.11.243 [VT]	unknown
N	54.170.123.99 [VT]	unknown
N	81.88.57.80 [VT]	unknown
N	96.16.88.180 [VT]	unknown
N	54.68.182.72 [VT]	unknown
N	34.213.106.51 [VT]	unknown
N	65.1.152.134 [VT]	unknown
N	43.250.140.2 [VT]	unknown
N	66.102.1.27 [VT]	unknown

pincho en Suricata alerts, para analizar las alertas de Suricata:

cape Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex Search

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

[PCAP](#) [PCAP](#)

Hosts (846) DNS (3724) TCP (10652) UDP (5093) HTTP (3082) SMTP (0) IRC (0) ICMP (218) Suricata Alerts (464) Suricata TLS (0) Suricata HTTP (0) Suricata Files (0)

Suricata Alerts

Timestamp	Source IP	Source Port	Destination IP	Destination Port	Protocol	GID	SID	REV	Signature	Category	Severity
2023-12-01 17:48:14.816490+0000	192.168.122.6 [VT]	52560	8.8.4.4 [VT]	53	UDP	1	2027758	2	ET DNS Query for .cc TLD	Potentially Bad Traffic	2
2023-12-01 17:49:01.285568+0000	192.36.38.33 [VT]	443	192.168.122.6 [VT]	49319	TCP	1	2522317	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 318	Misc Attack	2
2023-12-01 17:49:14.364054+0000	178.20.55.16 [VT]	443	192.168.122.6 [VT]	49332	TCP	1	2520030	4032	ET TOR Known Tor Exit Node Traffic group 31	Misc Attack	2
2023-12-01 17:49:14.364054+0000	178.20.55.16 [VT]	443	192.168.122.6 [VT]	49332	TCP	1	2522030	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 31	Misc Attack	2
2023-12-01 17:49:21.232403+0000	165.227.174.150 [VT]	9001	192.168.122.6 [VT]	49315	TCP	1	2522229	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 230	Misc Attack	2
2023-12-01 17:50:21.749237+0000	192.36.38.33 [VT]	443	192.168.122.6 [VT]	49319	TCP	1	2522317	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 318	Misc Attack	2
2023-12-01 17:50:44.584435+0000	192.168.122.6 [VT]	49556	192.185.105.154 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2
2023-12-01 17:50:45.423017+0000	192.168.122.6 [VT]	49493	3.33.130.190 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2
2023-12-01 17:50:50.343837+0000	192.168.122.6 [VT]	49461	188.114.97.5 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2
2023-12-01 17:50:53.571793+0000	192.168.122.6 [VT]	49852	192.185.105.154 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2
2023-12-01 17:50:57.625779+0000	192.168.122.6 [VT]	49901	104.26.14.11 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2
2023-12-01 17:50:59.138594+0000	192.168.122.6 [VT]	50148	3.33.130.190 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2
2023-12-01 17:50:59.726471+0000	192.168.122.6 [VT]	50166	192.185.105.154 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2

los TCP de destino:

cape

Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

[PCAP](#) [PCAP](#)

Hosts (846) DNS (3724) TCP (10852) UDP (5093) HTTP (3082) SMTP (0) IRC (0) ICMP (218) Suricata Alerts (464) Suricata TLS (0) Suricata HTTP (0) Suricata Files (0)

Source	Source Port	Destination	Destination Port
192.168.122.6	49269	34.94.245.237	80
192.168.122.6	49271	104.198.2.251	80
192.168.122.6	49272	34.143.166.163	80
192.168.122.6	49273	34.143.166.163	80
192.168.122.6	49274	91.215.85.17	80
192.168.122.6	49276	95.86.30.3	80
192.168.122.6	49319	192.36.38.33	443
192.168.122.6	49332	178.20.55.16	443
192.168.122.6	49338	185.183.194.90	443
192.168.122.6	49339	185.241.208.240	110
192.168.122.6	49341	190.12.87.61	80
192.168.122.6	49343	190.12.87.61	80
192.168.122.6	49346	190.12.87.61	80
192.168.122.6	49347	190.12.87.61	80

los UDP:

cape

Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

[PCAP](#) [PCAP](#)

Hosts (846) DNS (3724) TCP (10852) UDP (5093) HTTP (3082) SMTP (0) IRC (0) ICMP (218) Suricata Alerts (464) Suricata TLS (0) Suricata HTTP (0) Suricata Files (0)

Source	Source Port	Destination	Destination Port
192.168.122.6	63013	239.255.255.250	3702
192.168.122.6	50366	239.255.255.250	3702
192.168.122.6	62642	239.255.255.250	1900
192.168.122.6	137	192.168.122.255	137
192.168.122.6	62452	8.8.4.4	53
192.168.122.6	65148	8.8.8.8	53
192.168.122.6	65148	8.8.4.4	53
192.168.122.6	57427	8.8.4.4	53
192.168.122.6	64138	8.8.4.4	53
192.168.122.6	52560	8.8.4.4	53
192.168.122.6	138	192.168.122.255	138

en Dropped Files vemos los ficheros que se han creado en el sistema durante la ejecución del malware:

cape

Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex Search

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

File Name	state
File Type	ASCII text, with very long lines, with CRLF line terminators
Associated Filenames	C:\Users\ama\AppData\Local\Temp\4kPv6a\G8e\state
File Size	5363 bytes
MD5	46bb15cff6cd008502d3b369730a617a
SHA1	091538338113975f1d4fc5d78bd8f140395751b
SHA256	28d0f433206d8147c5e453754fe1c0123a6b564436afb37c2d310af0b7abc4a [VT] [MWDB] [Bazaar]
SHA3-384	e31c87879b568eff37979c778215d028ac301802e12cfda9749510eee0f3a3ffd09c1516058d76bc5857e573e675592
CRC32	8D9CB836
TLSH	T1F2B15C7D6288187C5C38BB6C16837C1AC407BCA01F1BF225E6696ED46A444277F062C
Ssdeep	48:cg+LZXQxTGRSuIMtcf1XHDWuIQQd4kXGaY2GE+J1Z4xV2obrspmH1pN2wQ7zikDraS8nXHDWuIQQgkFVW++iYUswQPKD

File Name	state
File Type	ASCII text, with very long lines, with CRLF line terminators
Associated Filenames	C:\Users\ama\AppData\Local\Temp\4kPv6a\G8e\state

el análisis de memoria, lo tengo apagado

cape

Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex Search

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

Sorry! No Memory details.

Back to the top

CAPE Sandbox on GitHub

los procesos dampeados:

cape

Dashboard Recent Pending Search API Submit Statistics Docs Changelog

Search term as regex

Quick Overview Behavioral Analysis Network Analysis Dropped Files (50) Memory Analysis Process Dumps (22) Payloads (38) Comments Compare this analysis to...

File Name	0d297c0f7cde6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f32d
File Type	PE32+ executable (GUI) x86-64, for MS Windows
File Size	2871808 bytes
Process	explorer.exe
PID	7040
Path	C:\Windows\explorer.exe
MD5	e5ce02472c553582599a01ccab6eda2f
SHA1	7b0625260c54426bedffee48fbefbb946266bc342
SHA256	0d297c0f7cde6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f32d [VT] [MWDB] [Bazaar]
SHA3-384	323be2ca90bb6b9cbd0d7cc3e87419230d1839fc1fb78125ac63cd21ed4c05d59641fa98565e6c2ace5c43d4a6720cfc
CRC32	D6284E30
TLSH	T1EDD5AE42FB605AE1D06B8935C462CB72D771FC4126145B1F2690FB5B6FB32E16B2A38C
Ssdeep	49152 cxcelJlIRYaisQhfCUyovYYYYYYYYYYRYYYYYYYYYYE3IA7eFUJN9qjoso2WurZlWRvYYYYYYYYYYRYYYYYYYYY