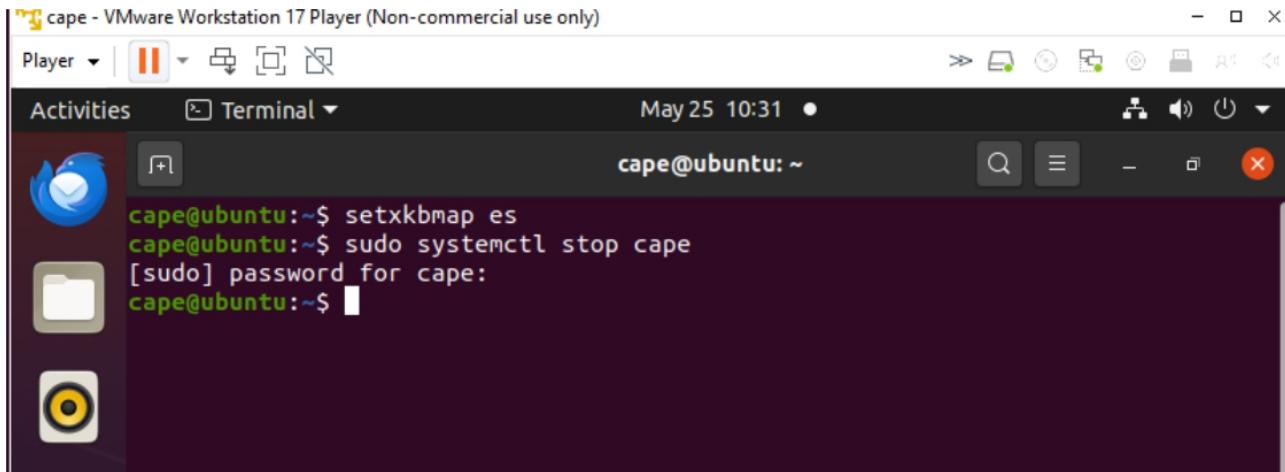


ANÁLISIS DE MALWARE

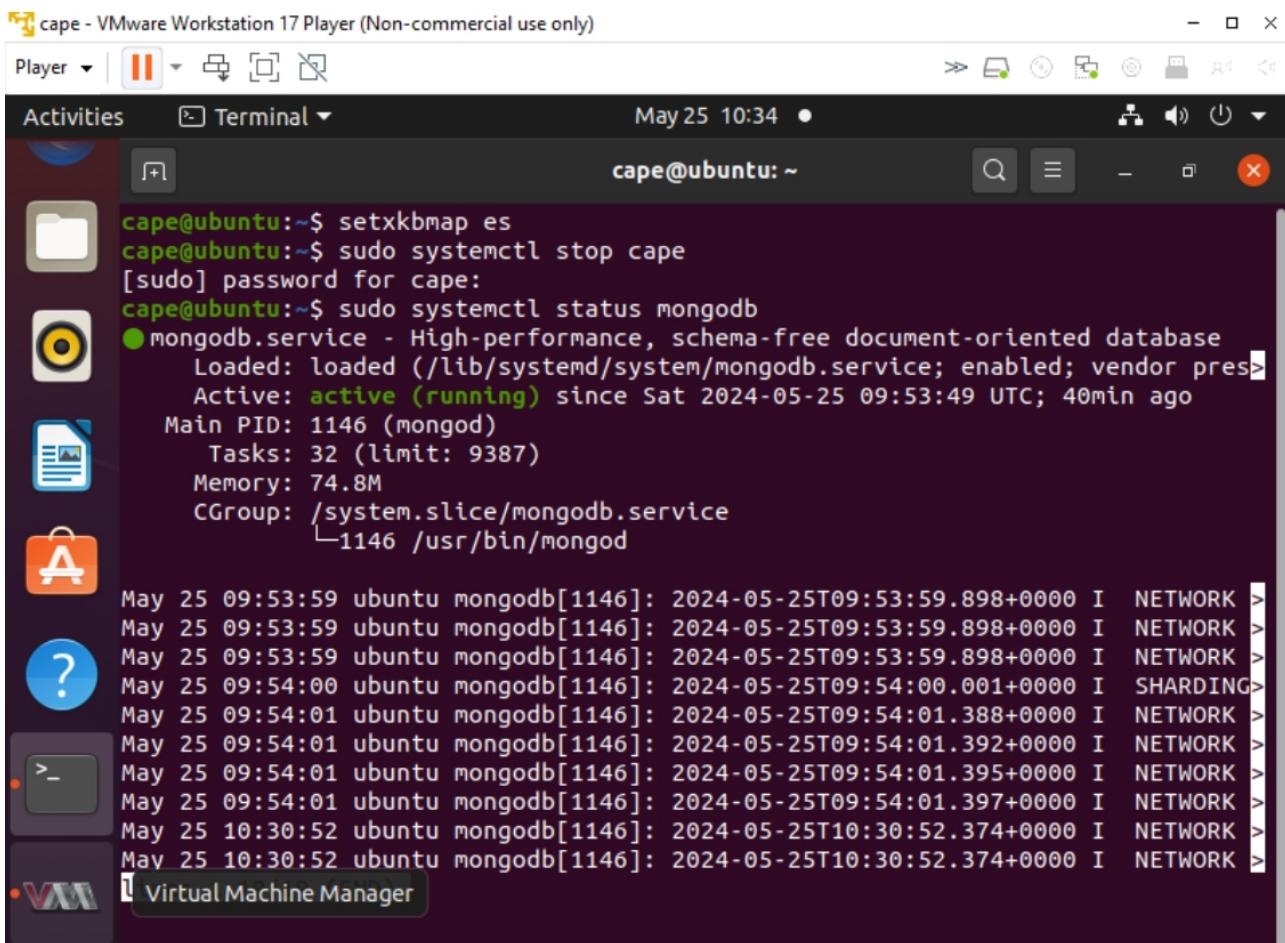
Primero realizo unas comprobaciones de que los servicios funcionan:

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

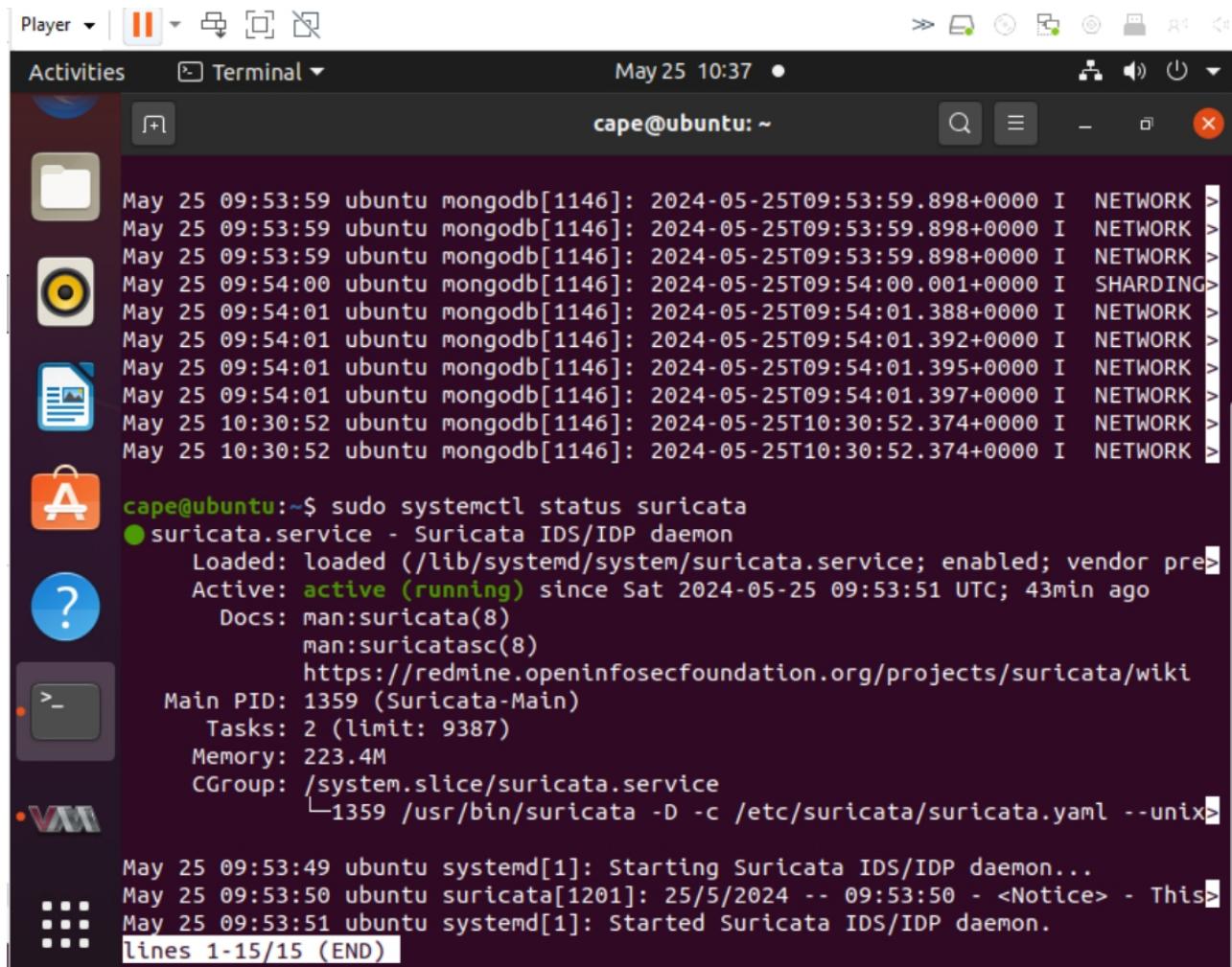


```
cape@ubuntu:~$ setxkbmap es
cape@ubuntu:~$ sudo systemctl stop cape
[sudo] password for cape:
cape@ubuntu:~$ sudo systemctl status mongodb
● mongodb.service - High-performance, schema-free document-oriented database
   Loaded: loaded (/lib/systemd/system/mongodb.service; enabled; vendor pres
     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

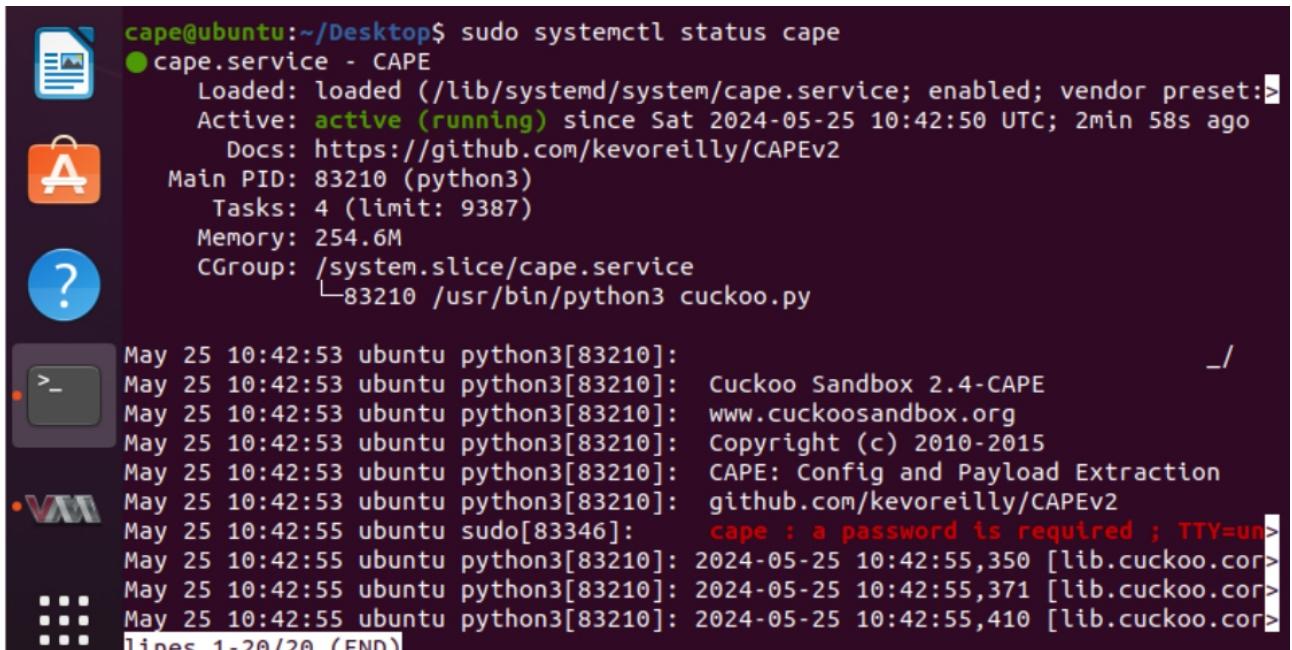
```
cape@ubuntu:~/Desktop/$ cd Desktop/
cape@ubuntu:~/Desktop$ ./tcpdump_user.sh
cape@ubuntu:~/Desktop$
```

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)
```

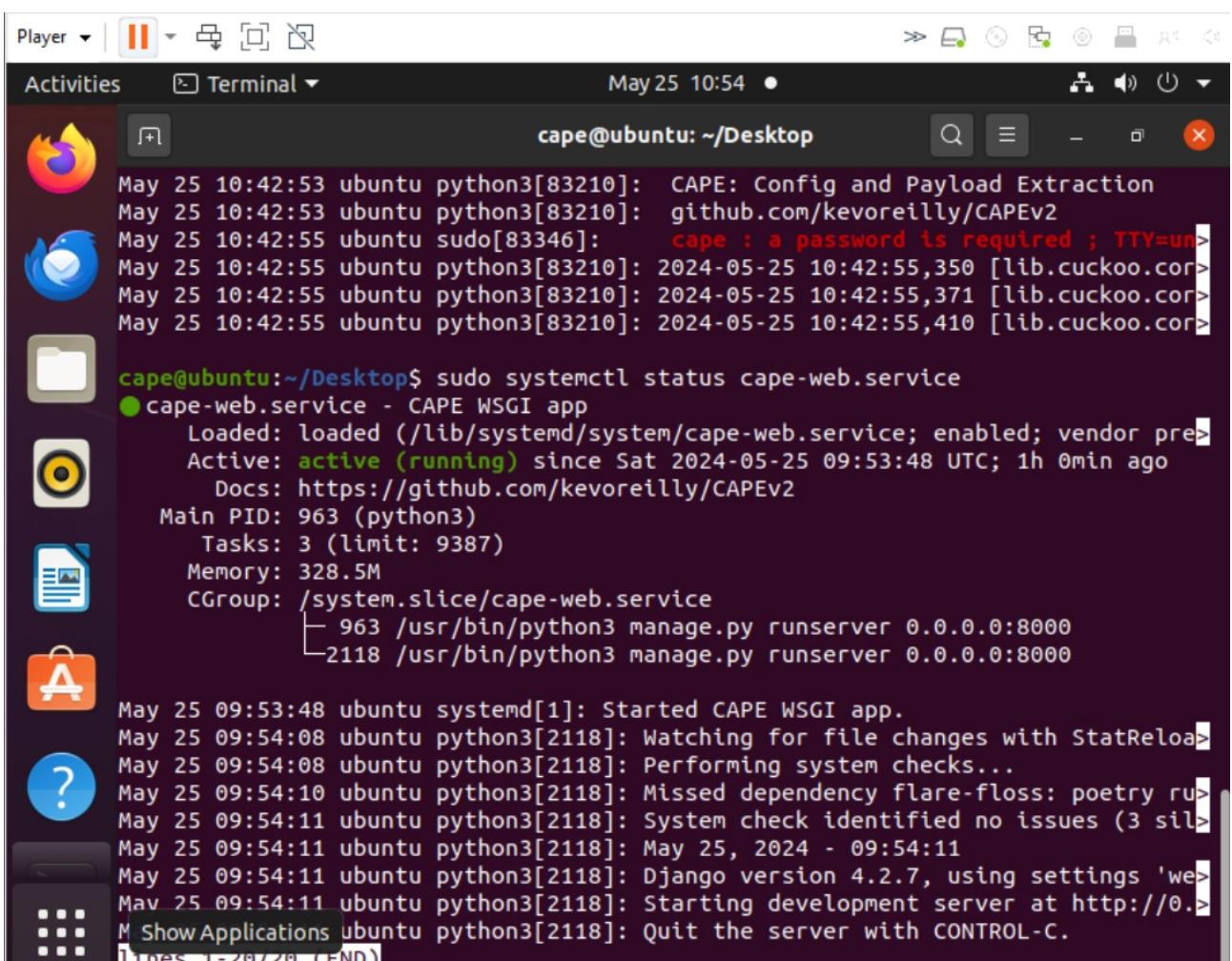
compruebo el cape normal



```
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

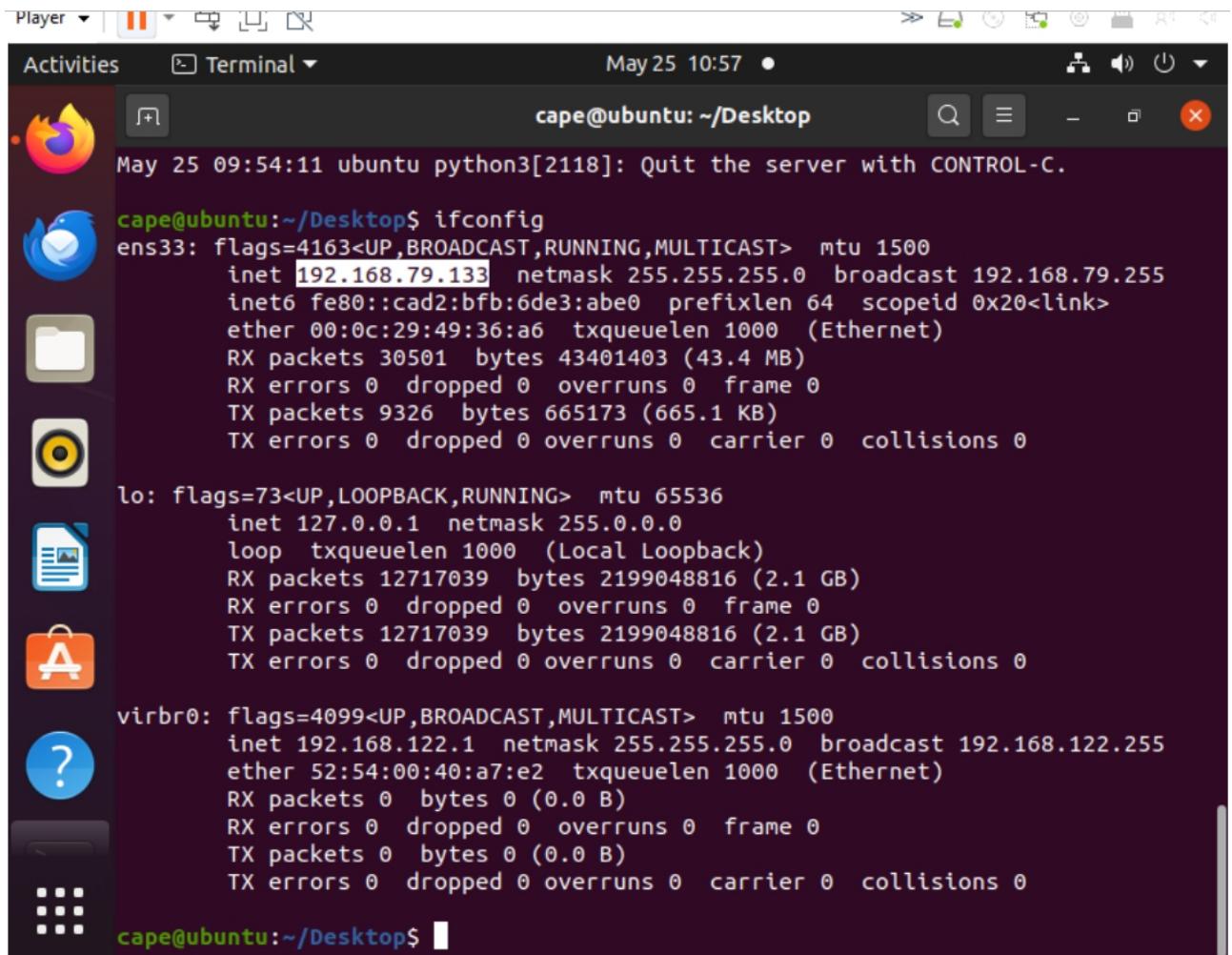
cape@ubuntu:~/Desktop$ sudo systemctl status cape-web.service
● cape-web.service - CAPE WSGI app
   Loaded: loaded (/lib/systemd/system/cape-web.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-05-25 09:53:48 UTC; 1h 0min ago
     Docs: https://github.com/kevoreilly/CAPEv2
     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 of the command is displayed, listing network interfaces (ens33, lo, virbr0) with their flags, MTU, and IP configurations. The IP address 192.168.79.133 is clearly visible under the ens33 interface.

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

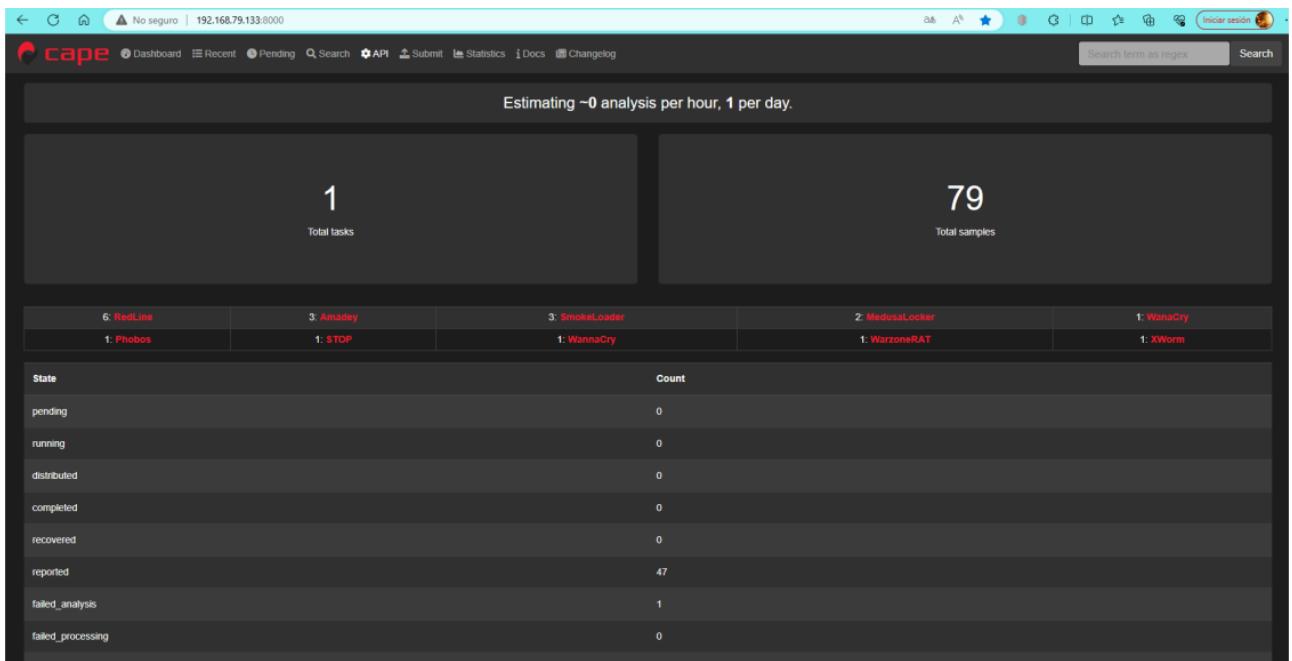
cape@ubuntu:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.79.133 netmask 255.255.255.0 broadcast 192.168.79.255
        inet6 fe80::cad2:bfb:6de3:abe0 prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:49:36:a6 txqueuelen 1000 (Ethernet)
            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 anfitrón 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:

The screenshot shows the Cape interface with the "Recent" tab selected. Sample ID 73 is highlighted. The table below provides detailed information about the sample:

ID	Timestamp	Machine	Package	Filename	MD5	Detections	Task tags	SunAlert				PCAP	ClamAV	Status
								PK G	HTTP/TLS/F	VT	MalScore			
80	2023-12-02 00:18:14	win7	exe	3928.exe	ebe783ba2f8e3fd2da2bded27eced	SmokeLoader	false	exe	0/-/-/-	-	10.0	PCAP	-	reported
79	2023-12-02 00:12:37	win7	exe	B65B.exe	33a60439e95fbdfc10016075f97aeab0c	SmokeLoader	false	exe	0/-/-/-	-	10.0	PCAP	-	reported
78	2023-12-01 23:44:18	win7	exe	quasarRAT.bat.exe	92f44e405db16ae55d97e3bfe3b132fa		false	exe	0/-/-/-	-	1.0	PCAP	-	reported
77	2023-12-01 23:12:58	win7	exe	XClient.exe	e47a5d191f0acb69797087ab43b24370	XWorm		exe	0/-/-/-	-	1.0	PCAP	-	reported
76	2023-12-01 23:28:23	win7	generic	quasarRAT.bat	09a47e33c5bcc69ef1d6a34bb966197d			gen	0/-/-/-	-	0.0	PCAP	-	reported
75	2023-12-01 22:51:43	win7	exe	e5372acb761bf91bed6.exe	887e0e9454a36659cd7a0dd94425c1e			exe	0/-/-/-	-	1.0	PCAP	-	reported
74	2023-12-01 16:17:02	win7	exe	1100b4580e6299445e00a5c2	54ecd7b2d5a1a4e14160c7812efa1237			exe	0/-/-/-	-	2.0	PCAP	-	reported
73	2023-12-01 16:09:47	win7	exe	82d763b6c97ca40a29.exe	fc5c9eb057d45f5f578593342ed53	SmokeLoader		exe	464/-/-/-	-	10.0	PCAP	-	reported
72	2023-12-01 17:45:13	win7	exe	1100b4580e6299445e00.exe	54ecd7b2d5a1a4e14160c7812efa1237			exe	0/-/-/-	-	1.0	PCAP	-	reported
71	2023-12-01 17:17:11	win7	lnk	forelouper.lnk	c49299cd978aa9c6a1938e59033bd3b8		false	lnk	0/-/-/-	-	1.0	PCAP	-	reported

esta es la pantalla de la muestra 73

The screenshot shows the cape analysis interface. At the top, it displays 'No seguro | 192.168.79.133:8000/analysis/73/'. Below the header, there's a navigation bar with links like Dashboard, Recent, Pending, Search, API, Statistics, Docs, and Changelog. A search bar at the top right includes 'Search term as regex' and a 'Search' button.

The main content area has tabs for Quick Overview, Behavioral Analysis, Network Analysis, Dropped Files (50), Memory Analysis, Process Dumps (22), Payloads (38), Comments, and Compare this analysis to... The 'Quick Overview' tab is selected.

Below the tabs, a message says 'Detection(s): SmokeLoader'. The 'Analysis' section contains tables for 'Category' (FILE, exe) and 'Machine' (win7). The 'File Details' section shows the file name as '82d765b6cd97ca240529.exe' and the file type as '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						
Name	Label	Manager	Started On	Shutdown On	Route	
win7	win7	KVM	2023-12-01 17:45:13	2023-12-01 18:09:46		internet

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

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
0x00040000	0x00003749	0x00054a86	0x00054a86	5.0	C:\src64\ryexofavutlx-pazzadidzopoga25-wowurugjbuher78ib.pdb	2022-12-05 15:35:42	1756ec87e9180426f96d9ce779d24407		24a118ed3241d13007f0bf74a4479cc	31b0e7b0995cc97ed9db659f75ab3b69	40d8dac2b2aaa2b0
Version Infos											
FileDescription											
Malling											
LegalCopyright											
Copyright (C) 2022, Crazy											
OriginalFilename											
Mangler											
ProductsVersion											
19.3.71.61											
ProductionVersion											
16.28.79.2											
Translation											
0x25ad 0xe0e92											

en la sección Sections

Sections						
Name	RAW Address	Virtual Address	Virtual Size	Size of Raw Data	Characteristics	Entropy
.text	0x00000400	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	fc5e9eb857d45fa5f578593342ede53
SHA1	6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c
SHA256	82d763b6cd97ca240a291c90b8de517232b92bbe5b593549a61547a30eebf19 [VT] [MWDB] [Bazaar]
SHA3-384	30a9a95df9dcff5c2ad741b0aef60ff675de999d8338d6e9e640583cf26061518734b52562ea050542b9fffe159660b
CRC32	296CEADF
TLSH	T15164F85382F1BD44E9268B729F2FE6EC775DF6508FB776922189E1F40B1172C263B10
Ssdeep	3072.FH+D6UjSY7Oy4kzCEuCBtly5utlg9vcYST5GzGNIZUX558.56Utx7Oy42BojCIsa22A
PE	<input type="button" value="File"/> <input type="button" value="Strings"/> <input type="button" value="VirusTotal"/>

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
0x00400000	0x00004a86	0x00054a86	0x00054a86	5.0	C:\sl64_nyexofavubxpuzadidzopoga25-wowurugibuhen7\lib.pdb	2022-12-05 15:35:42	1756ec87e918042696d9ce779d24407		24af18ed3241d13d0706ff74a4479cc	31b3e7b0995cc97ed9db659f75ab3b69	40d8da2b2aa2b0
Version Infos											
FileVersion	Malling	LegalCopyright	Copyright (C) 2022, Crazy	OriginalFilename	Humper	ProductsVersion	19.3.71.61	ProductionVersion	16.78.79.2	Translation	0x25ad 0x0e92

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
<ul style="list-style-type: none"> T1033 - System Owner/User Discovery <ul style="list-style-type: none"> encrypt_pcinfo T1082 - System Information Discovery <ul style="list-style-type: none"> antvm_generic_dlskreg recon_fingerprint antvm_generic_bios antvm_generic_system T1010 - Application Window Discovery <ul style="list-style-type: none"> antidebug_windows T1083 - File and Directory Discovery <ul style="list-style-type: none"> antemu_winedefend T1497 - Virtualization/Sandbox Evasion <ul style="list-style-type: none"> antvm_generic_dlskreg antvm_generic_system antvm_generic_bios antvm_vbox_keys antemu_winedefend T1057 - Process 	<ul style="list-style-type: none"> T1003 - OS Credential Dumping <ul style="list-style-type: none"> infostealer_mail infostealer_browser T1106 - Native API <ul style="list-style-type: none"> process_creation_suspicious_location antidebug_guardprocess T1539 - Steal Web Session Cookie <ul style="list-style-type: none"> infostealer_cookie T1555 - Credentials from Password Stores <ul style="list-style-type: none"> infostealer_browser T1552 - Unsecured Credentials <ul style="list-style-type: none"> infostealer_mail infostealer_browser T1555_003 - Credentials from Web Browsers <ul style="list-style-type: none"> infostealer_browser T1552_001 - Credentials in Files <ul style="list-style-type: none"> infostealer_mail infostealer_browser 	<ul style="list-style-type: none"> T1129 - Shared Modules <ul style="list-style-type: none"> dropper T1106 - Native API <ul style="list-style-type: none"> process_creation_suspicious_location antidebug_guardprocess T1059_001 - PowerShell <ul style="list-style-type: none"> powershell_download powershell_inject T1560 - Archive Collected Data <ul style="list-style-type: none"> encrypt_pcinfo 	<ul style="list-style-type: none"> T1114 - Email Collection <ul style="list-style-type: none"> infostealer_mail 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_autoun T1560 - Archive Collected Data <ul style="list-style-type: none"> encrypt_pcinfo 	<ul style="list-style-type: none"> T1547 - Boot or Logon Autostart Execution <ul style="list-style-type: none"> persistence_autoun T1055 - Process Injection <ul style="list-style-type: none"> injection_inter_process explorer_http T1547_001 - Registry Run Keys / Startup Folder <ul style="list-style-type: none"> persistence_autoun 	<ul style="list-style-type: none"> T1547 - Boot or Logon Autostart Execution <ul style="list-style-type: none"> persistence_autoun T1218_004 - InstallUtil spawns_dev_util T1202 - Indirect Command Execution <ul style="list-style-type: none"> suspicious_comm_and_tools uses_windows_utils T1562 - Impair Defenses <ul style="list-style-type: none"> ansisandbox_uinfo T1036 - Masquerading <ul style="list-style-type: none"> explorer_http T1055 - Process Injection <ul style="list-style-type: none"> injection_inter_process explorer_http T1218 - System Binary Proxy Execution <ul style="list-style-type: none"> spawns_dev_util T1112 - Modify Registry <ul style="list-style-type: none"> persistence_autoun powershell_download T1070 - Indicator Removal 	<ul style="list-style-type: none"> T1071 - Application Layer Protocol <ul style="list-style-type: none"> stealth_window T1218_004 - InstallUtil spawns_dev_util T1202 - Indirect Command Execution <ul style="list-style-type: none"> suspicious_comm_and_tools uses_windows_utils T1562 - Impair Defenses <ul style="list-style-type: none"> ansisandbox_uinfo T1036 - Masquerading <ul style="list-style-type: none"> explorer_http T1055 - Process Injection <ul style="list-style-type: none"> injection_inter_process explorer_http T1218 - System Binary Proxy Execution <ul style="list-style-type: none"> spawns_dev_util T1112 - Modify Registry <ul style="list-style-type: none"> persistence_autoun powershell_download T1070 - Indicator Removal 	<ul style="list-style-type: none"> T1496 - Data Encrypted for Impact <ul style="list-style-type: none"> ransomware_file_modifications T1485 - Data Destruction <ul style="list-style-type: none"> anomalous_delete_file 	

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.

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

The screenshot shows the cape behavioral analysis interface. At the top, there's a navigation bar with links for Dashboard, Recent, Pending, Search, API, Statistics, Docs, and Changelog. A search bar is also present. Below the navigation, there are tabs for Quick Overview, Behavioral Analysis (which is selected), Network Analysis, Dropped Files (50), Memory Analysis, Process Dumps (22), Payloads (38), Comments, and Compare this analysis to... The main content area displays a 'Process Tree' and a 'Command History'. The Process Tree shows a hierarchy of processes, starting from a root file (82d763bcd97ca240a29.exe) and branching down to various system processes like explorer.exe, cmd.exe, and tasklist.exe. The Command History section lists numerous commands run by the malware, such as 'cmd /k cmd < Enjoyed & exit', 'findstr /I "avastui.exe avgui.exe nswwscsvc.exe sophoshealth.exe"', and various file operations like copying files to the 'Infected + Tin + Excited + Condo 29768\Perceived' directory. The interface has a clean, modern design with a dark header and light body.

aquí veo las órdenes que ha lanzado al sistema windows:

cape Dashboard Recent Pending Search API Submit Statistics Docs Changelog

cmd.exe (6048) Perceived.pdf (4668) PING EXE (6328) svchost.exe (6592) sppsvc.exe (1088) svchost.exe (976) WerFault.exe (5376) ACF7.exe (2256) taskhost.exe (1896)

82d763b6cd97ca240a29.exe, PID: 772, Parent PID: 2344
Full Path: C:\Users\lma\AppData\Local\Temp\82d763b6cd97ca240a29.exe
Command Line: "C:\Users\lma\AppData\Local\Temp\82d763b6cd97ca240a29.exe"

default registry filesystem network process threading services device synchronization crypto browser all

Additional Filters

1

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 6	0x778c3046 0x778e13d2	NtQueryValueKey	KeyHandle: 0x00000000 ValueName: DisableUserModeCallbackFilter FullName: DisableUserModeCallbackFilter	failed	INVALID_HANDLE	2 times
2023-12-01 15:41:32.108	103 6	0x004060ec 0x0040374e	GetSystemTimeAsFileTime		SUCCESS	0x00000000	2 times
2023-12-01 15:41:32.108	103 6	0x0040609a 0x0040363e	HeapCreate	Options: 0 InitialSize: 0x00001000 MaximumSize: 0x00000000	SUCCESS	0x06a00000	2 times
2023-12-01 15:41:32.108	103 6	0x00404d1d 0x00000000	LdrGetDllHandle	FileName: KERNEL32.DLL ModuleHandle: 0x75d20000	SUCCESS	0x00000000	2 times
2023-12-01 15:41:32.108	103 6	0x00404d40 0x00000000	LdrGetProcAddress	ModuleName: kernel32.dll ModuleHandle: 0x75d20000 FunctionName: #1\$alloc 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

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 (5053) 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:

los TCP de destino:

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

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 17:49:01.285558+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]	50186	192.185.105.154 [VT]	22	TCP	1	2003068	7	ET SCAN Potential SSH Scan OUTBOUND	Attempted Information Leak	2

los UDP:

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

The screenshot shows the cape malware analysis interface. At the top, there's a navigation bar with links for Dashboard, Recent, Pending, Search, API, Submit, Statistics, Docs, and Changelog. A search bar is also present. Below the navigation, there are tabs for Quick Overview, Behavioral Analysis, Network Analysis, Dropped Files (50), Memory Analysis, Process Dumps (22), Payloads (38), Comments, and Compare this analysis to... The Dropped Files tab is selected.

Dropped Files (50) Details:

File Name	state
File Type	ASCII text, with very long lines, with CRLF line terminators
Associated Filenames	C:\Users\ama\AppData\Local\Temp\4kPv6aJG8e\state
File Size	5363 bytes
MD5	46bb15cffccdd08502d3b0369730a617a
SHA1	091538338113975f1d4fc5d78bd814f0395751b
SHA256	28d0f433205d81147c5e453754fe1c0123a6b564436ab37c2d310af0b7abc4a [VT] [MWD8] [Bazaar]
SHA3-384	e31c87879b5f58eff7979c778215d028ac301802e12cda9749510ee03a3fd09c1516058d76bc5857e573e675592
CRC32	8D9CB836
TLSH	T1F2B15C7DF628B187C5C38BB6C16837C1AC407BCA01F1BF225E6696ED46A444277F062C
Ssdeep	48cg+LZXQxTGRSuMTcf1XHDWuQD4kXGqY2GE+J1Z4xV2obrspmH1pNz2wQ7zikD.raS6nxDWuIQDgkfFWV++iYUSwQPkD

Below the file details, there are download buttons for PCAP and Text.

Network Analysis:

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

Below the network table, there are download buttons for PCAP and Text.

At the bottom of the interface, there are tabs for 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), and Suricata Files (0).

el análisis de memoria, lo tengo apagado

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...

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	0d297c0f7cd6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f32d
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	e5ce02472c5535b2599a01ccab6eda2f
SHA1	7b3625260c54426bedfee48fbefbb94626bb0c342
SHA256	0d297c0f7cd6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f32d [V1] [MVDB] [Bazaar]
SHA3-384	323be2ca90bb6b9cbd0d7cc3e87419230d1839fc1b78125ac63cd21ed4c05d59641fa98565e6c2ace5c43d4a6720cb
CRC32	D6284E30
TLSH	T1EDD5AE42FB605AE1D06B8935C462CB72D771FC4126145B1F2690FB5B6FB32E16B2A38C
Ssdeep	49152 cxceljIRYraisQhFCUyoYYYYYYYYYYRYYYYYYYYYYE3IA7/eFUJN9ejoso2WurcZlWrvYYYYYYYYYY RYYYYYYYYYYY
PE	PE
File	File
Strings	Strings
VirusTotal	VirusTotal