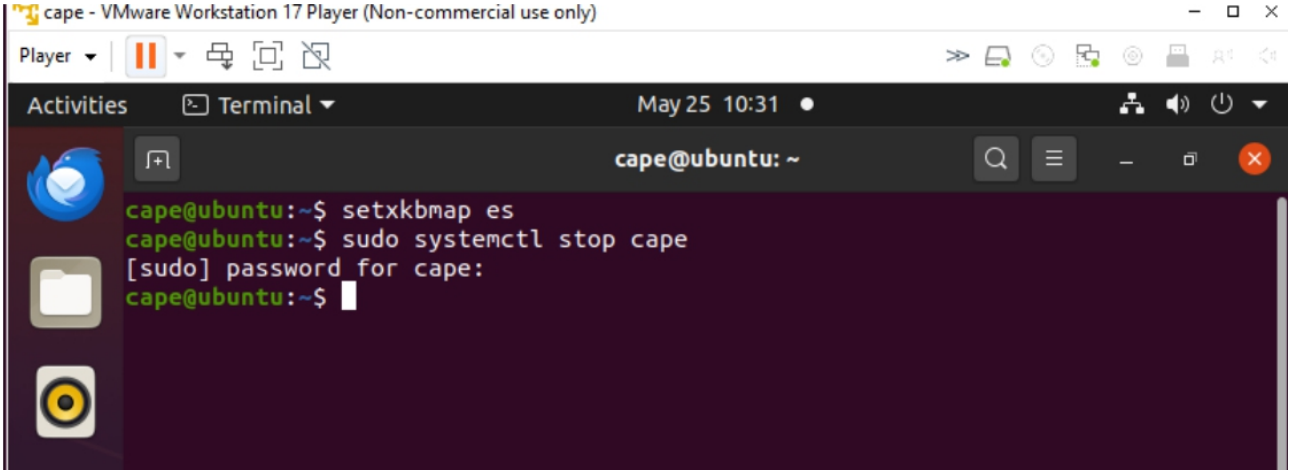
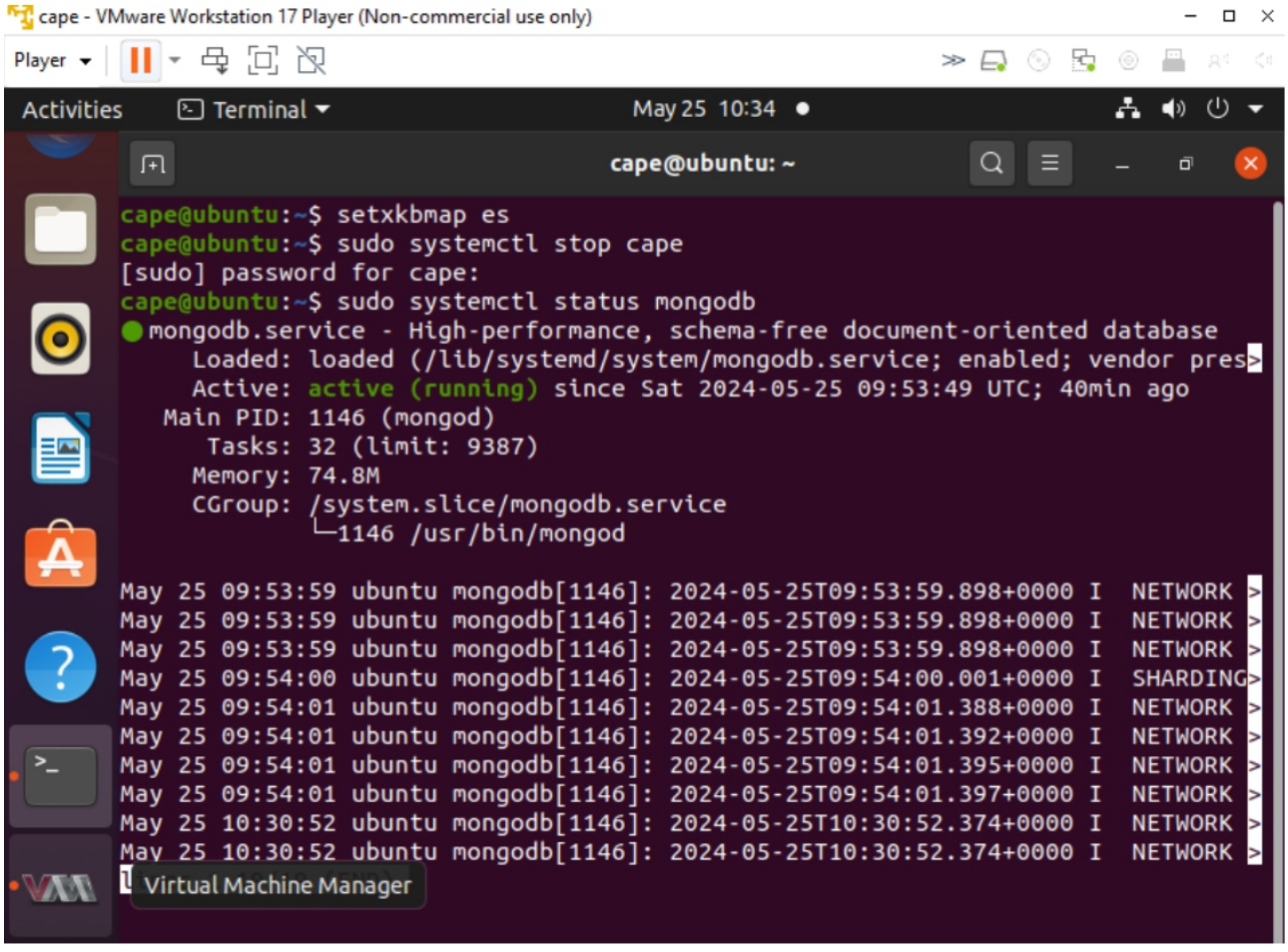
ANÁLISIS DE MALWARE

Primero realizo unas comprobaciones de que los servicios funcionan:

paro el servicio cape: sudo systemctl stop cape

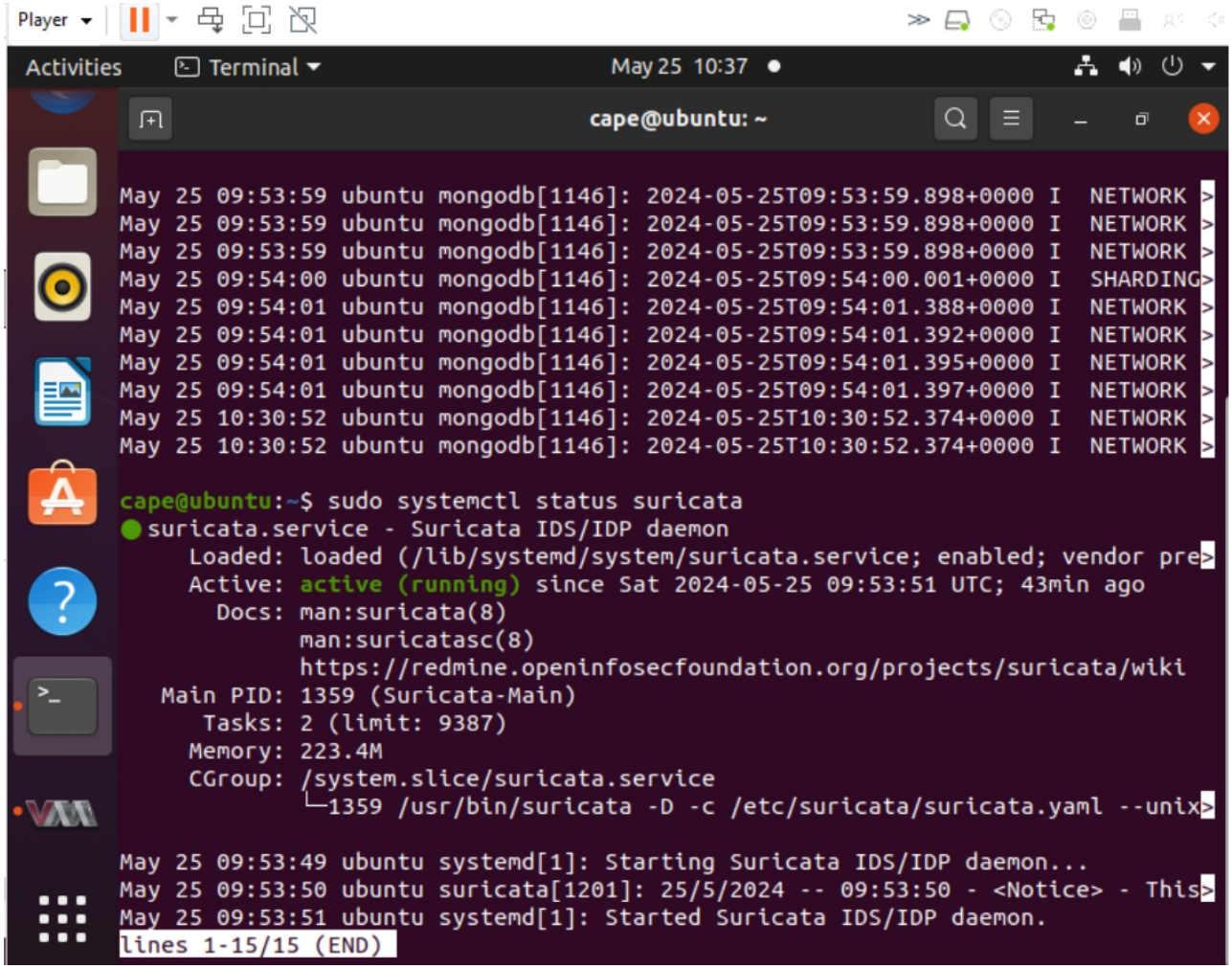


compruebo el estado de la bbdd mongodb: sudo systemctl status mongodb



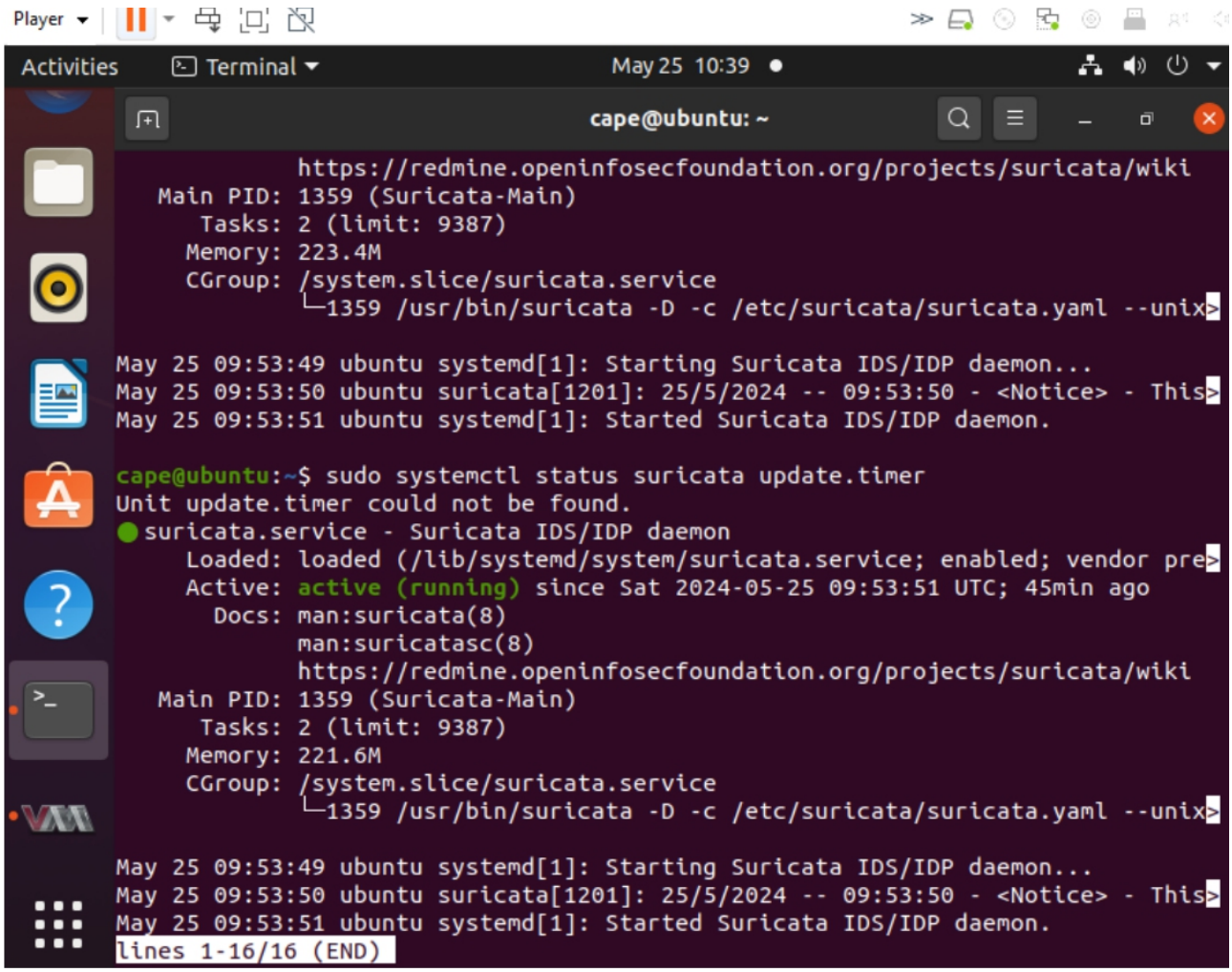
el active está en verde, con lo cual activa la bbdd

compruebo el estado de suricata: sudo systemctl status suricata

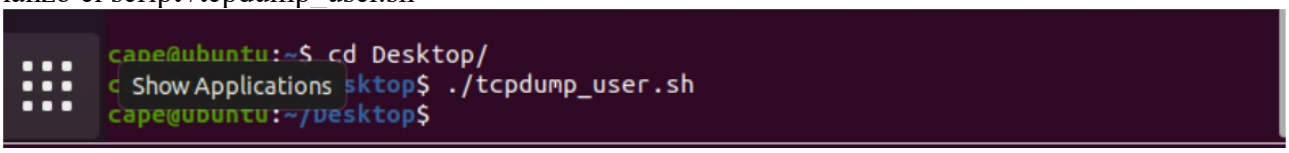


también está activa

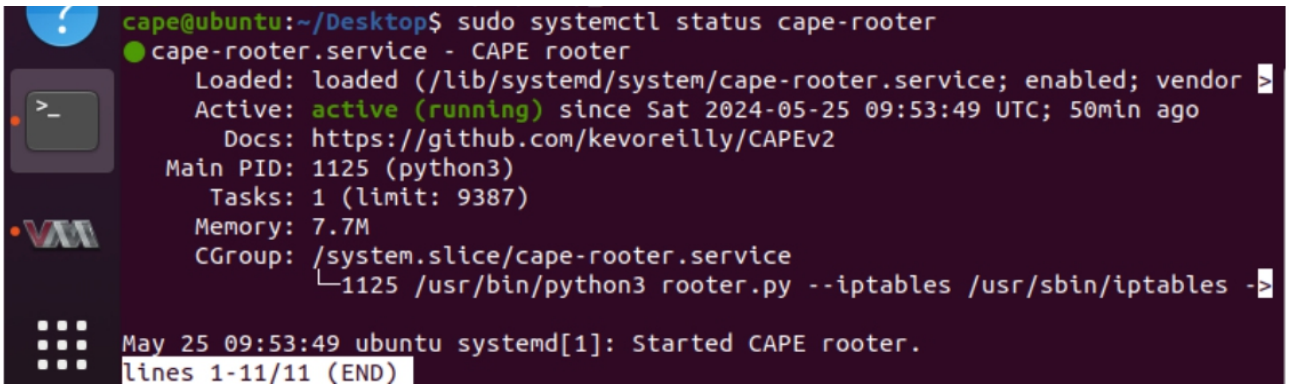
luego sudo systemctl status suricata update.timer



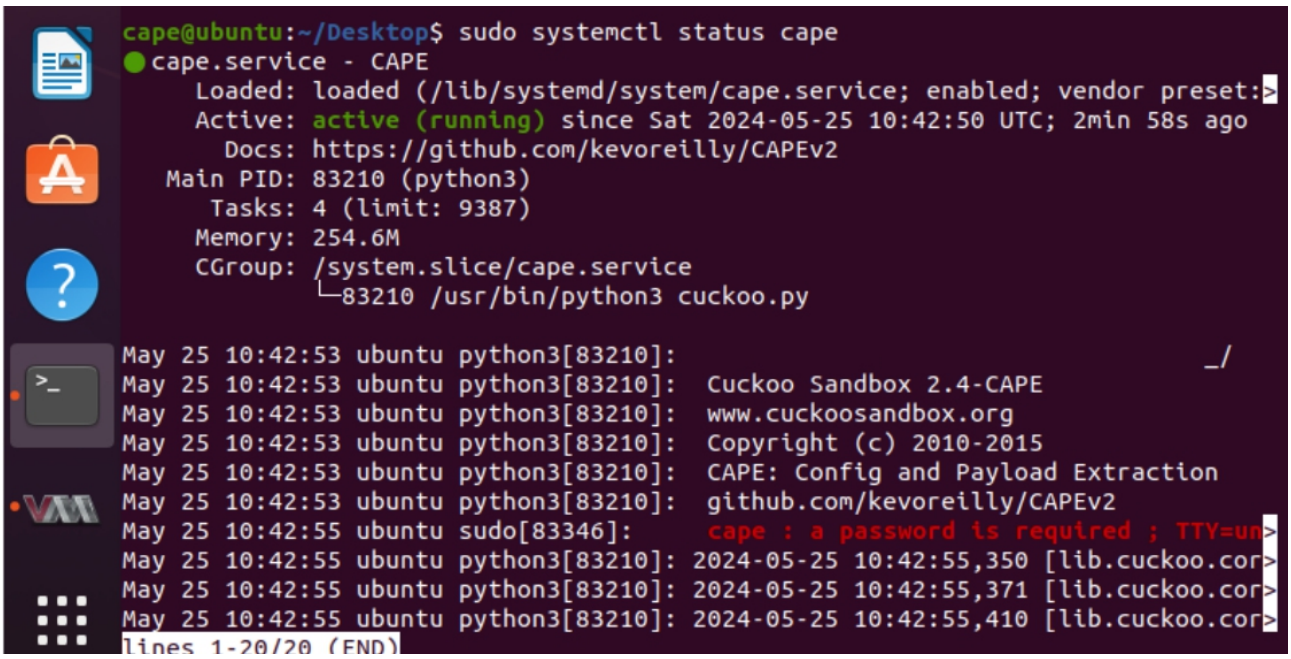
lanzo el script /tcpdump_user.sh



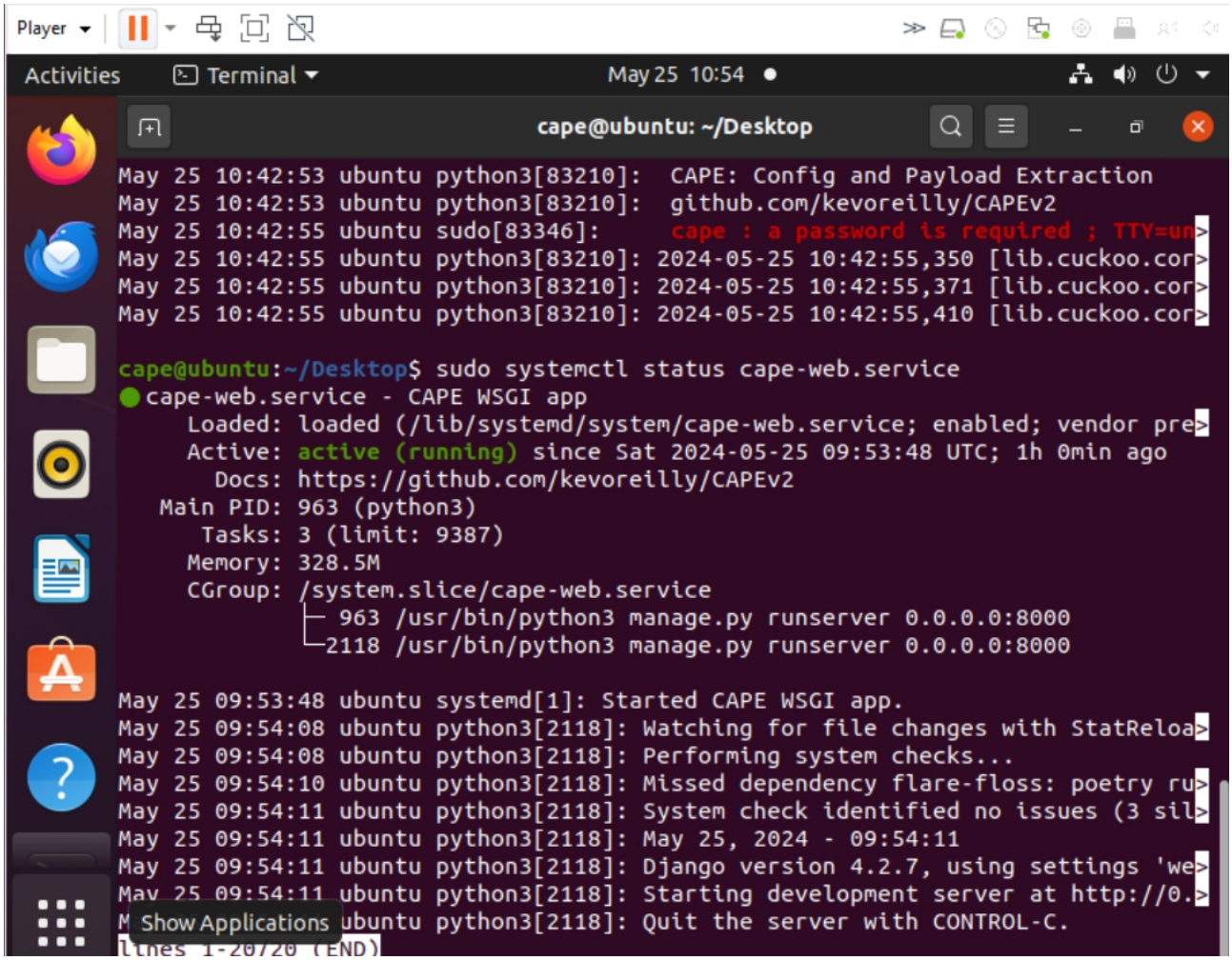
compruebo el cape-rooter



compruebo el cape normal



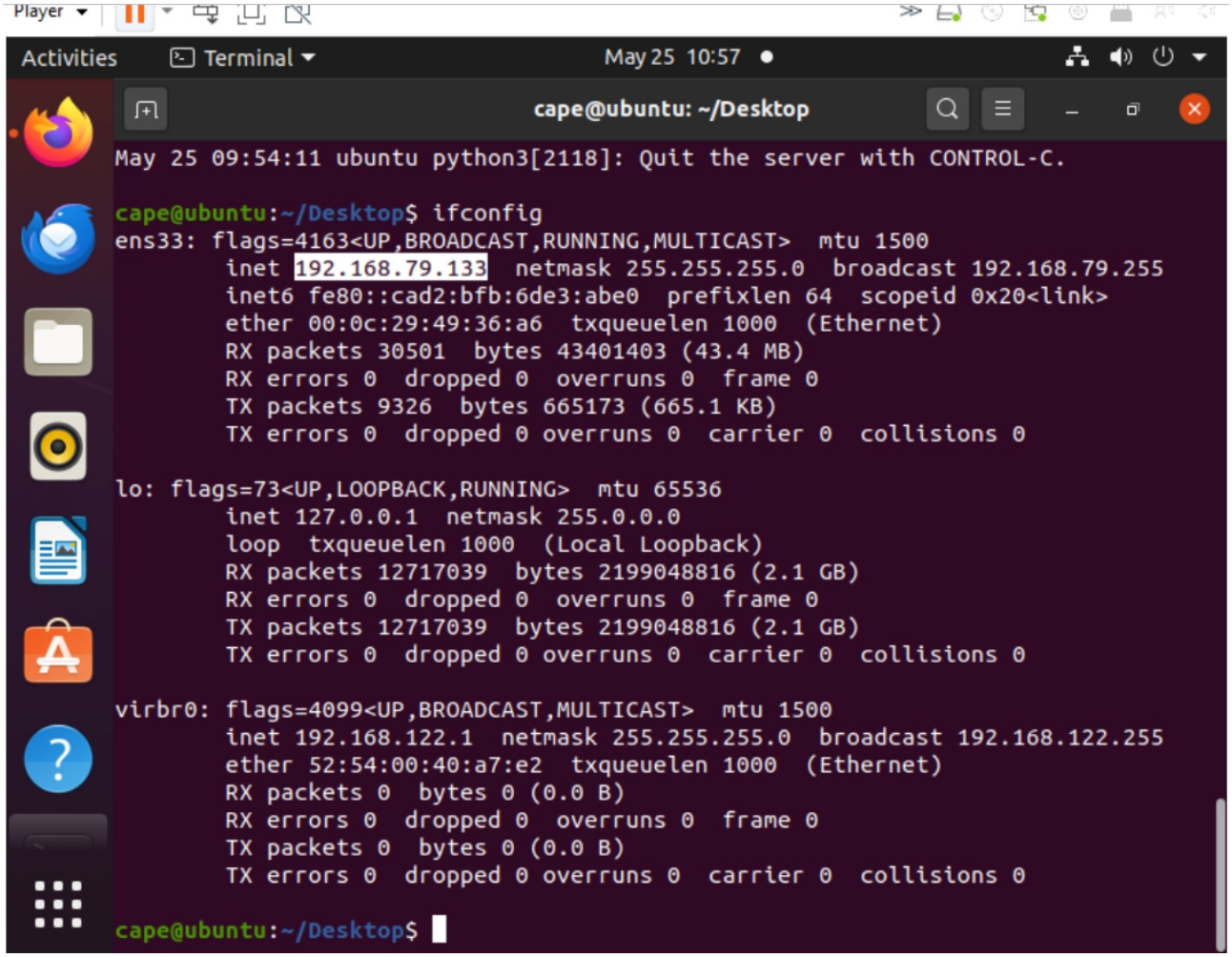
luego compruebo el cape web



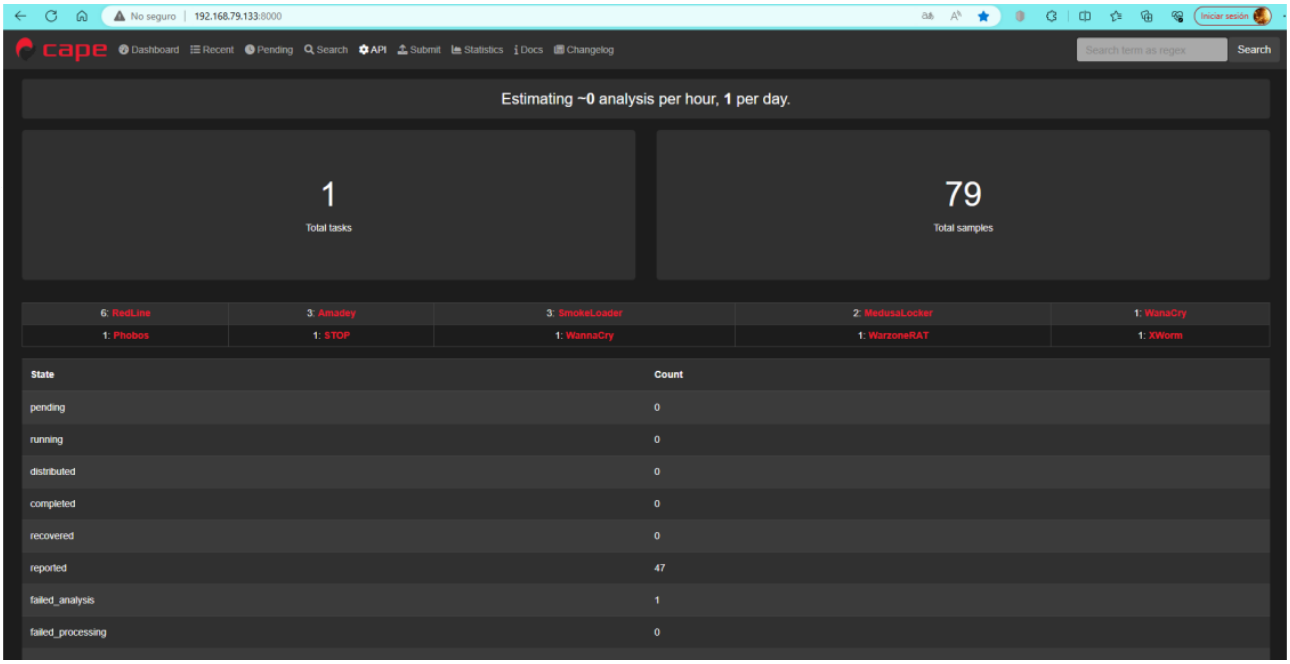
con estas comprobaciones me aseguro que todo está listo para analizar malware

ahora voy a la web:

copio mi ip

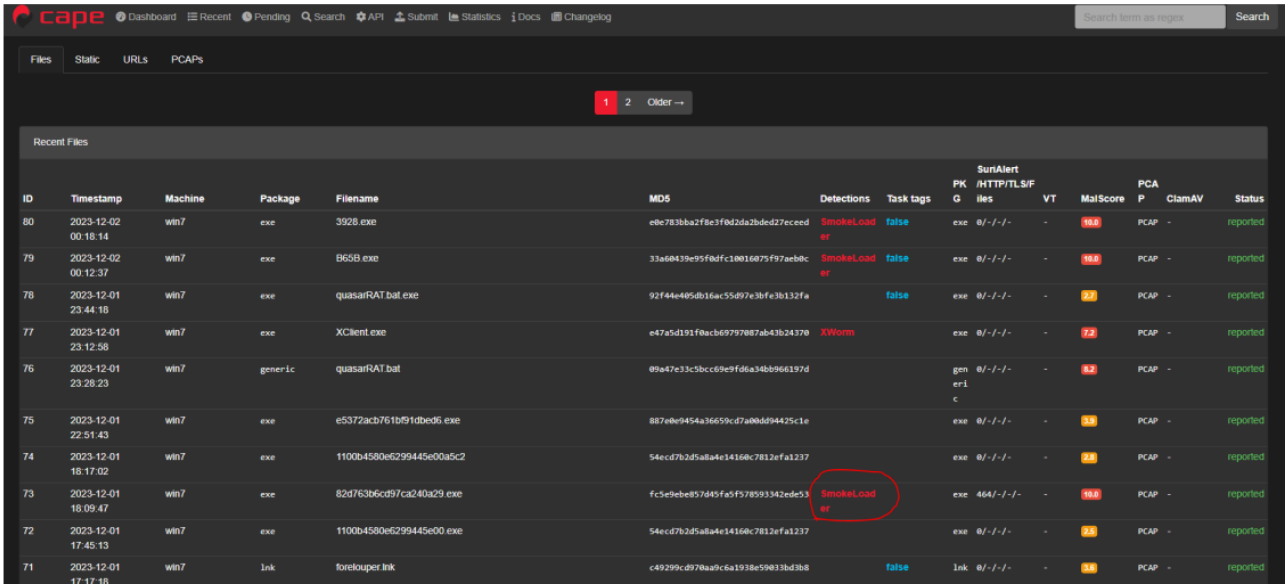


me voy al navegador de mi equipo anfitrión a la esa ip con puerto 8000

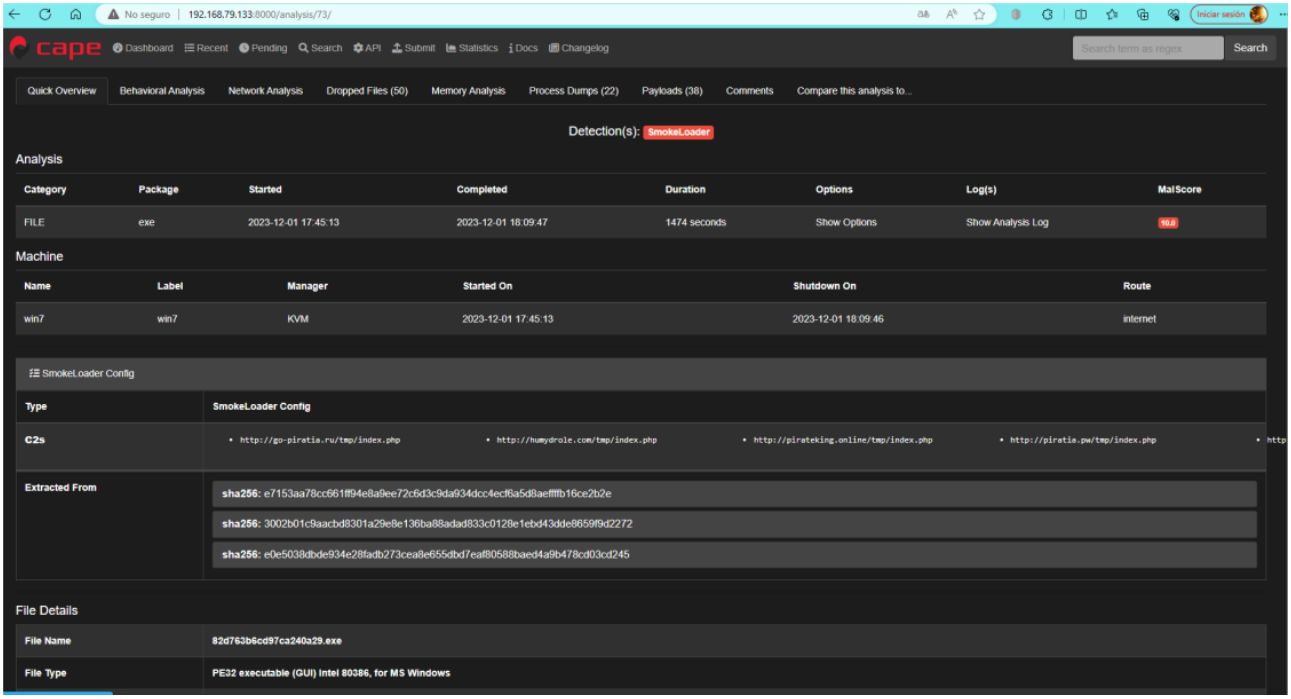


aquí tengo la interface de Cape con la que voy a analizar malware

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

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 codigo 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
0x00400000	0x00003749	0x00054a86	0x00054a86	5.0	C:\sir64_riyexofavubix-puzadidizopoga25-wowurugibuhen\78\b.pdb	2022-12-05 15:35:42	1756ec87e9180426f96d9ce779d24407		24a118ed3241d13d07f0bff74a4479cc	31b3e7b0995cc97ed9db659f75ab3b69	40d8dac2b2aaa2b0

Version Infos

FileDescription	Malling
LegalCopyright	Copyright (C) 2022, Crazy
OriginalFilename	Munpler
ProductsVersion	19.3.71.61
ProductionVersion	16.78.79.2
Translation	0x25ad 0x0e92

en la sección Sections

Sections

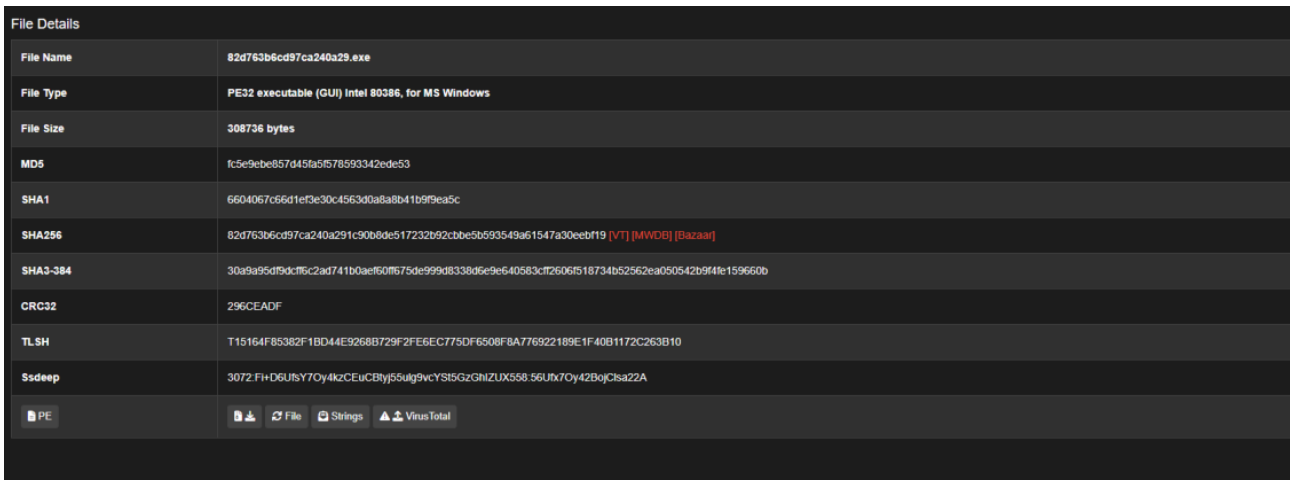
Name	RAW Address	Virtual Address	Virtual Size	Size of Raw Data	Characteristics	Entropy
.text	0x00000400	0x00001000	0x00028f56	0x00029000	IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ	6.84
.data	0x00029400	0x0002a000	0x0267557c	0x00001800	IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE	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:

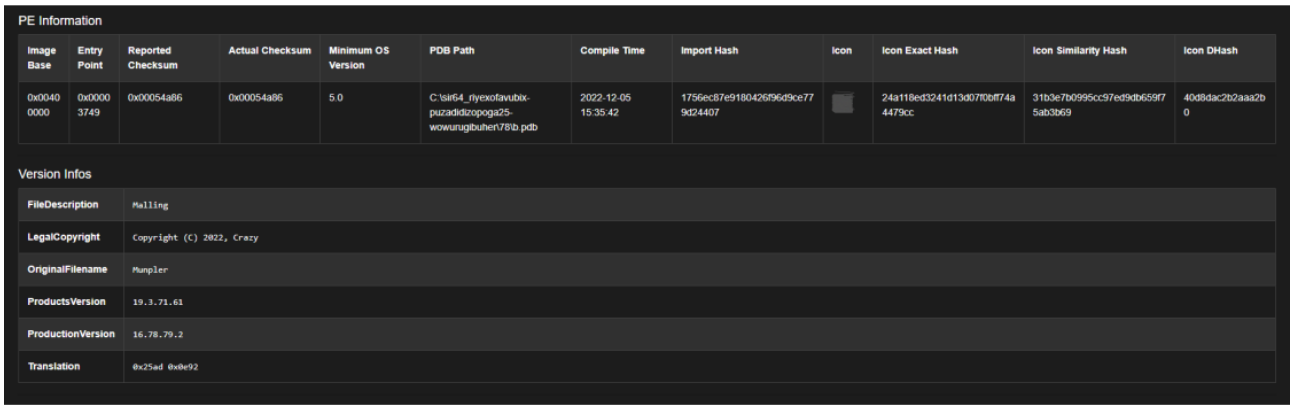
Kernel32: gestión ficheros, localiza en memoria las direcciones
User32: imprime mensaje
ADVAPI32: posible cifrado

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	fc5e9ebe857d45fa5f578593342ede53
SHA1	6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c
SHA256	82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19 [VT] [MWDB] [Bazaar]
SHA3-384	30a9a95df9dcff6c2ad741b0aef60ff675de999d8338d6e9e640583cff2606f518734b52562ea050542b9f4fe159660b
CRC32	296CEADF
TLSH	T15164F85382F1BD44E9268B729F2FE6EC775DF6508F8A776922189E1F40B1172C263B10
Ssdeep	3072:FI+D6UfsY7Oy4kzCEuCBtyj55ulg9vcYSt5GzGhlZUX558:56Ufx7Oy42BojCIsa22A
PE	File Strings VirusTotal



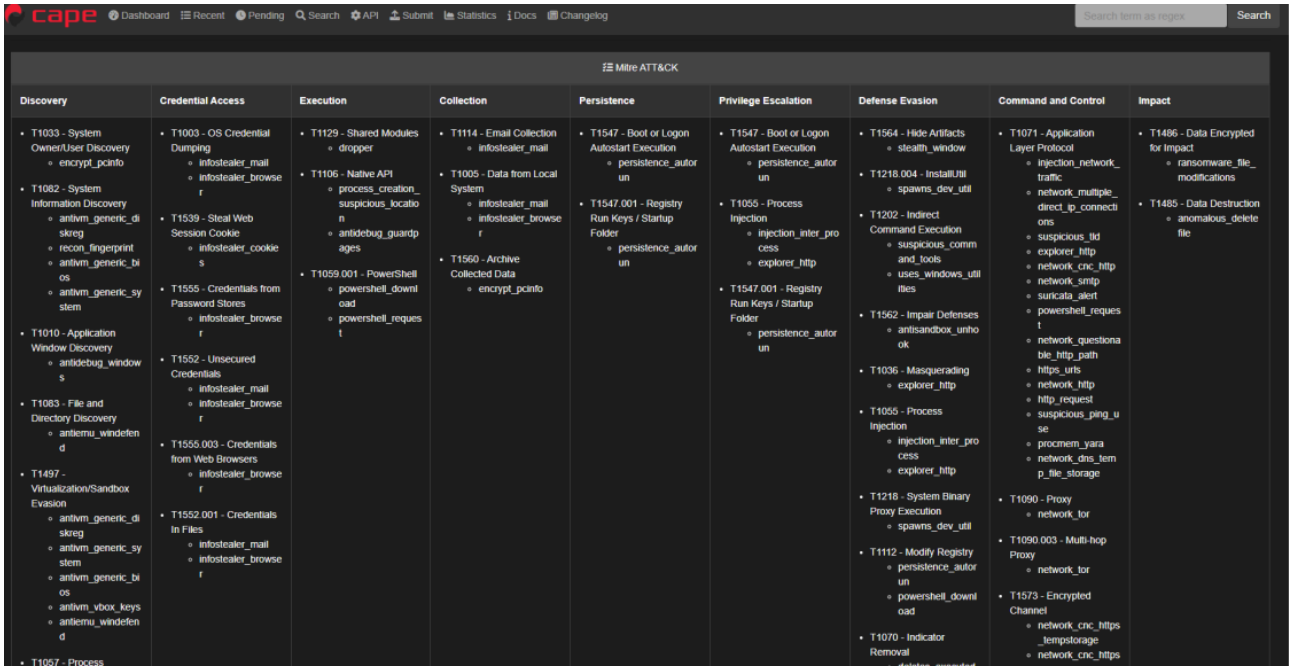
PE Information

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	0x00003749	0x00054a86	0x00054a86	5.0	C:\sir64_rlyexofavubix-puzadidizopoga25-wowurugibuhen\78\b.pdb	2022-12-05 15:35:42	1756ec87e9180426f96d9ce779d24407		24a118ed3241d13d07f0bff74a4479cc	31b3e7b0995cc97ed9db659f75ab3b69	40d8dac2b2aaa2b0

Version Infos

FileDescription	Mulling
LegalCopyright	Copyright (C) 2022, Crazy
OriginalFilename	Munpler
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:



cape Dashboard Recent Pending Search API Submit Statistics Docs Changelog Search

Mitre ATT&CK

Discovery
- T1033 - System Owner/User Discovery
  - encrypt_pcinfo
- T1082 - System Information Discovery
  - antivm_generic_diskreg
  - recon_fingerprint
  - antivm_generic_bios
  - antivm_generic_system
- T1010 - Application Window Discovery
  - antidebug_windows
- T1083 - File and Directory Discovery
  - antiemu_windefend
- T1497 - Virtualization/Sandbox Evasion
  - antivm_generic_diskreg
  - antivm_generic_system
  - antivm_generic_bios
  - antivm_vbox_keys
  - antiemu_windefend
- T1057 - Process

Credential Access
- T1003 - OS Credential Dumping
  - infostealer_mail
  - infostealer_browser
- T1539 - Steal Web Session Cookie
  - infostealer_cookies
- T1555 - Credentials from Password Stores
  - infostealer_browser
- T1552 - Unsecured Credentials
  - infostealer_mail
  - infostealer_browser
- T1555.003 - Credentials from Web Browsers
  - infostealer_browser
- T1552.001 - Credentials In Files
  - infostealer_mail
  - infostealer_browser

Execution
- T1129 - Shared Modules
  - dropper
- T1106 - Native API
  - process_creation_suspicious_location
  - antidebug_guardpages
- T1059.001 - PowerShell
  - powershell_download
  - powershell_request

Collection
- T1114 - Email Collection
  - infostealer_mail
- T1005 - Data from Local System
  - infostealer_mail
  - infostealer_browser
- T1560 - Archive Collected Data
  - encrypt_pcinfo

Persistence
- T1547 - Boot or Logon Autostart Execution
  - persistence_autorun
- T1547.001 - Registry Run Keys / Startup Folder
  - persistence_autorun

Privilege Escalation
- T1547 - Boot or Logon Autostart Execution
  - persistence_autorun
- T1055 - Process Injection
  - injection_inter_process
  - explorer_http
- T1547.001 - Registry Run Keys / Startup Folder
  - persistence_autorun

Defense Evasion
- T1564 - Hide Artifacts
  - stealth_window
- T1218.004 - InstallUtil
  - spawns_dev_util
- T1202 - Indirect Command Execution
  - suspicious_command_tools
  - uses_windows_utilities
- T1562 - Impair Defenses
  - antisandbox_unhook
- T1036 - Masquerading
  - explorer_http
- T1055 - Process Injection
  - injection_inter_process
  - explorer_http
- T1218 - System Binary Proxy Execution
  - spawns_dev_util
- T1112 - Modify Registry
  - persistence_autorun
  - powershell_download
- T1070 - Indicator Removal

Command and Control
- T1071 - Application Layer Protocol
  - injection_network_traffic
  - network_multiple_direct_ip_connections
  - suspicious_tld
  - explorer_http
  - network_cnc_http
  - network_smtp
  - suricata_alert
  - powershell_request
  - network_questionable_http_path
  - https_urls
  - network_http
  - http_request
  - suspicious_ping_use
  - procmem_yara
  - network_dns_temp_file_storage
- T1090 - Proxy
  - network_tor
- T1090.003 - Multi-hop Proxy
  - network_tor
- T1573 - Encrypted Channel
  - network_cnc_https_tempstorage
  - network_cnc_https

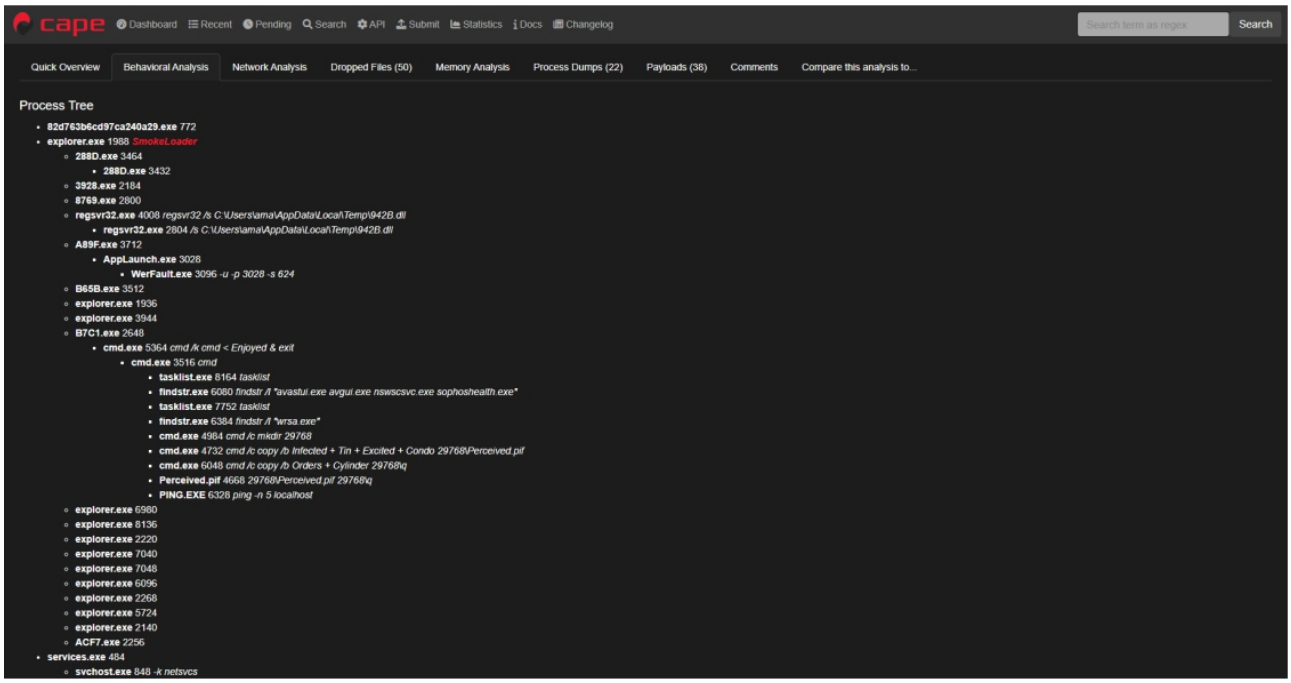
Impact
- T1486 - Data Encrypted for Impact
  - ransomware_file_modifications
- T1485 - Data Destruction
  - anomalous_delete file

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.

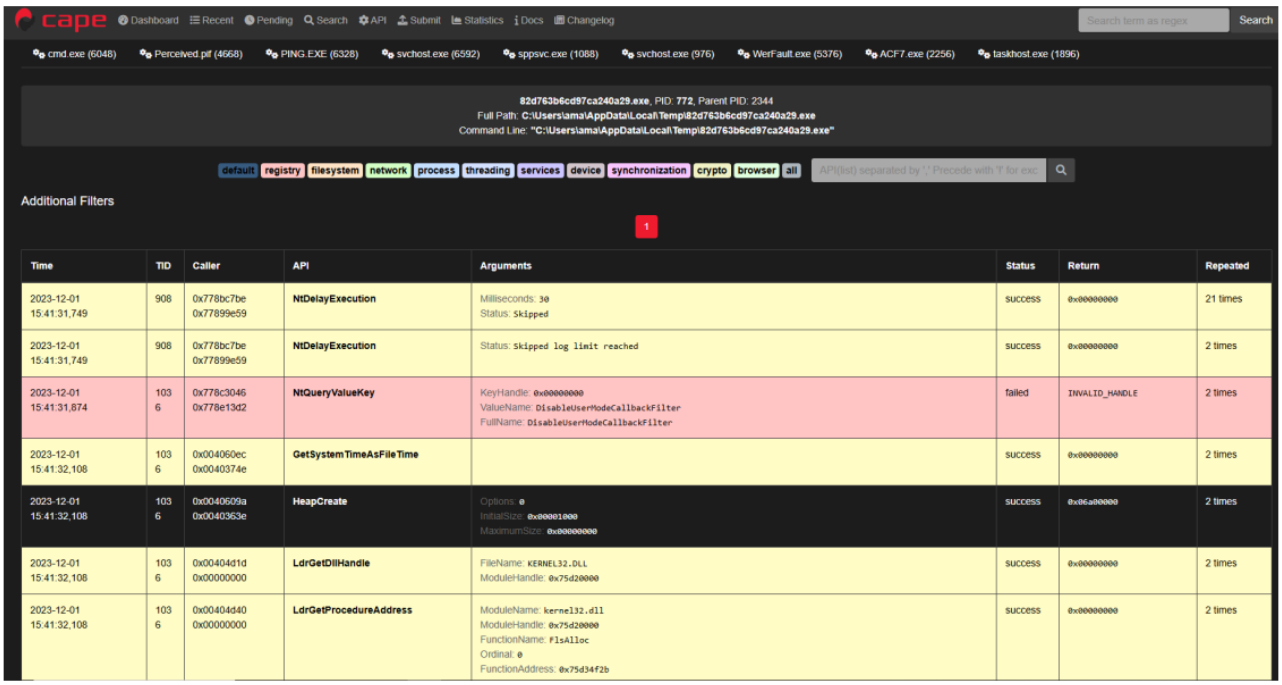
Collection: roba información de emails, datos del sistema local
Persistencia: crea persistencia al inicio del sistema, a través de claves de registro o de inicio.
Privilege Escalation: ejecución como system. Escalado de privilegios, como administrador.
Defense evasion: esconde ficheros en ruta, o los 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.

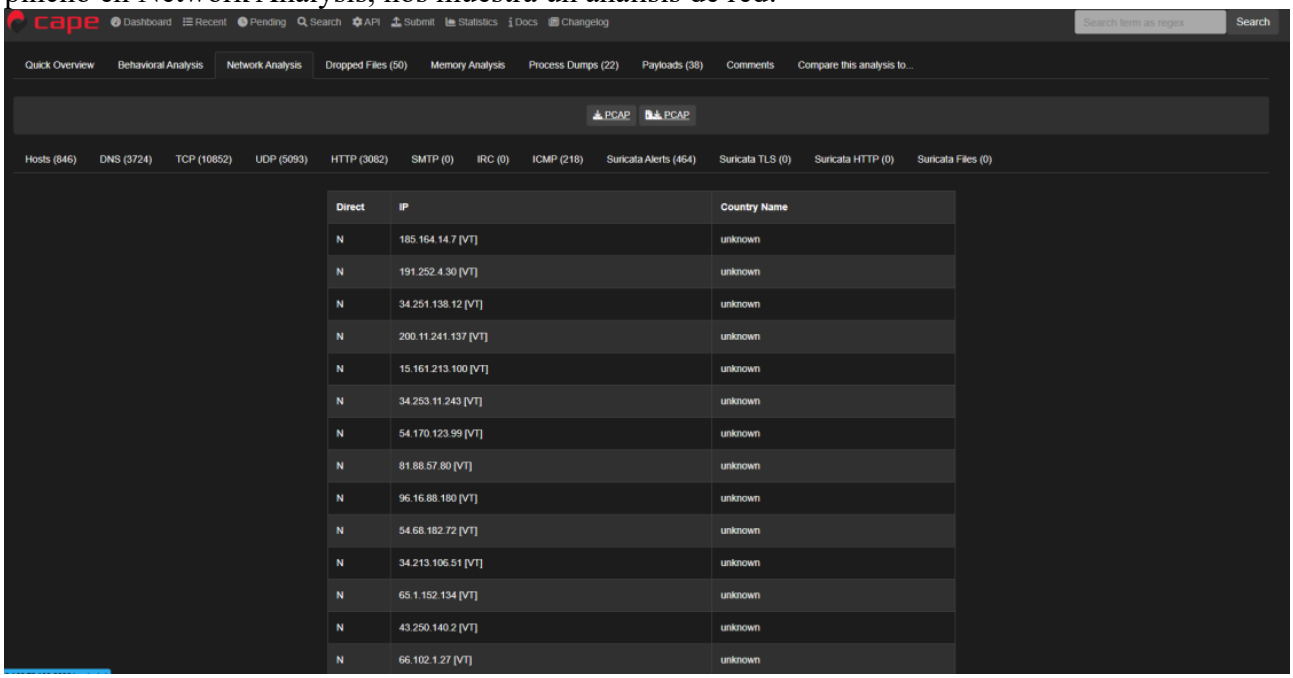
Pincho en Behavioral Analysis para observar el análisis de comportamiento del malware:



aquí veo las órdenes que ha lanzado al sistema windows:

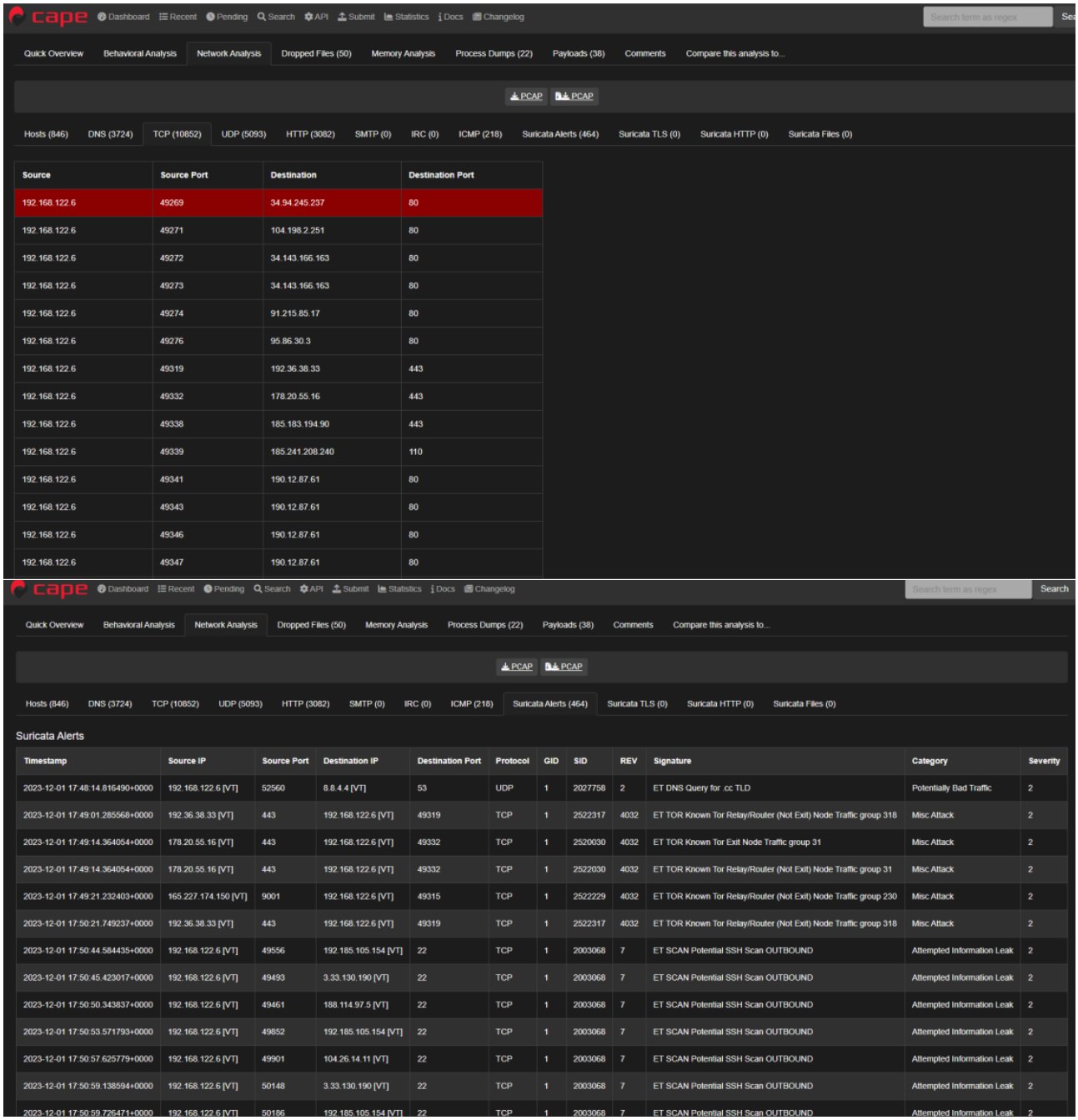


pincho en Network Analysis, nos muestra un análisis de red:



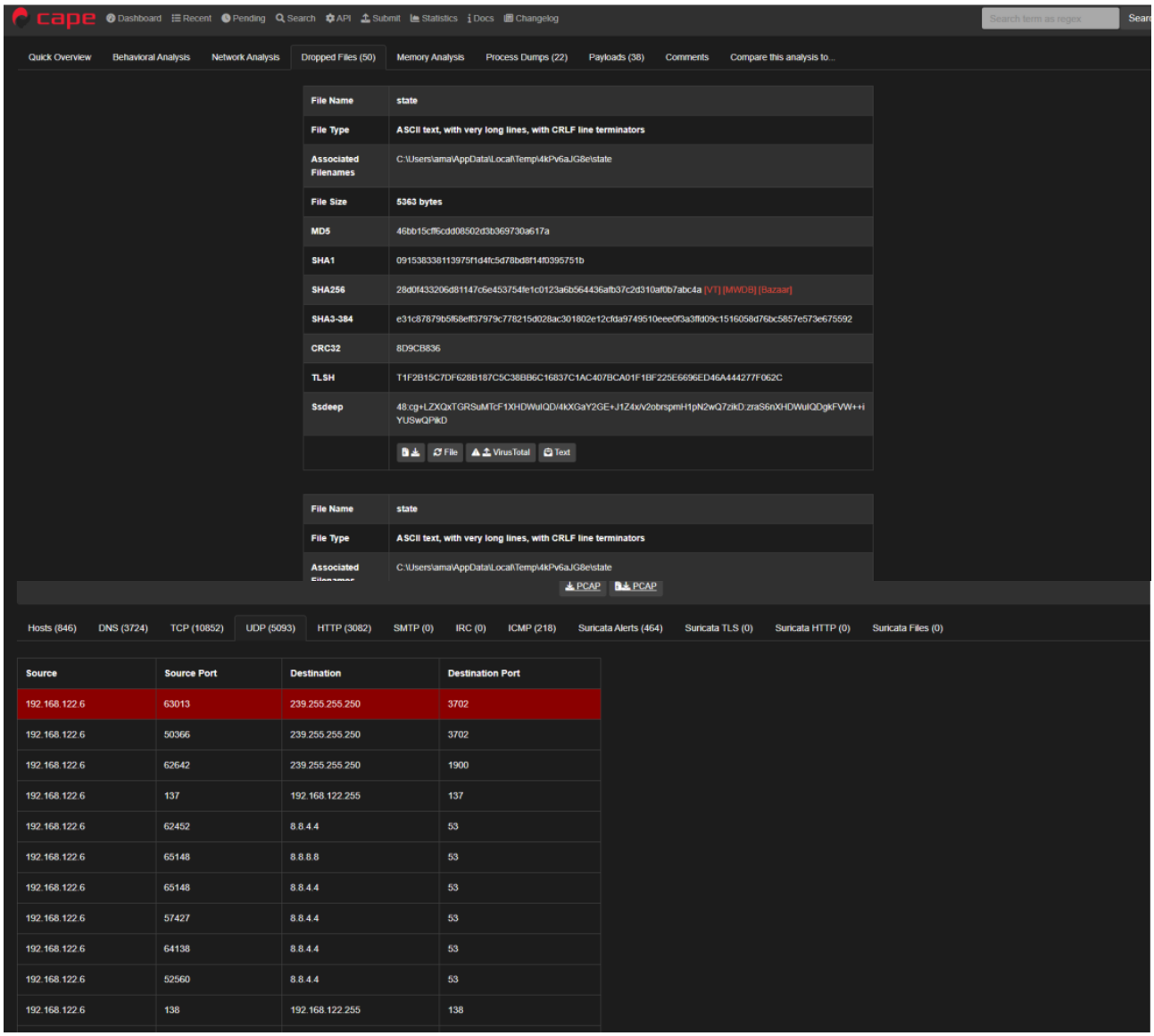
pincho en Suricata alerts, para analizar las alertas de Suricata:

los TCP de destino:

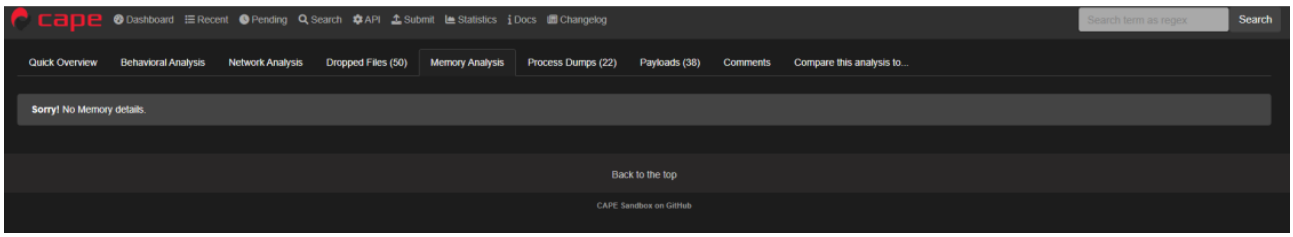


los UDP:

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



el análisis de memoria, lo tengo apagado



los procesos dampeados: