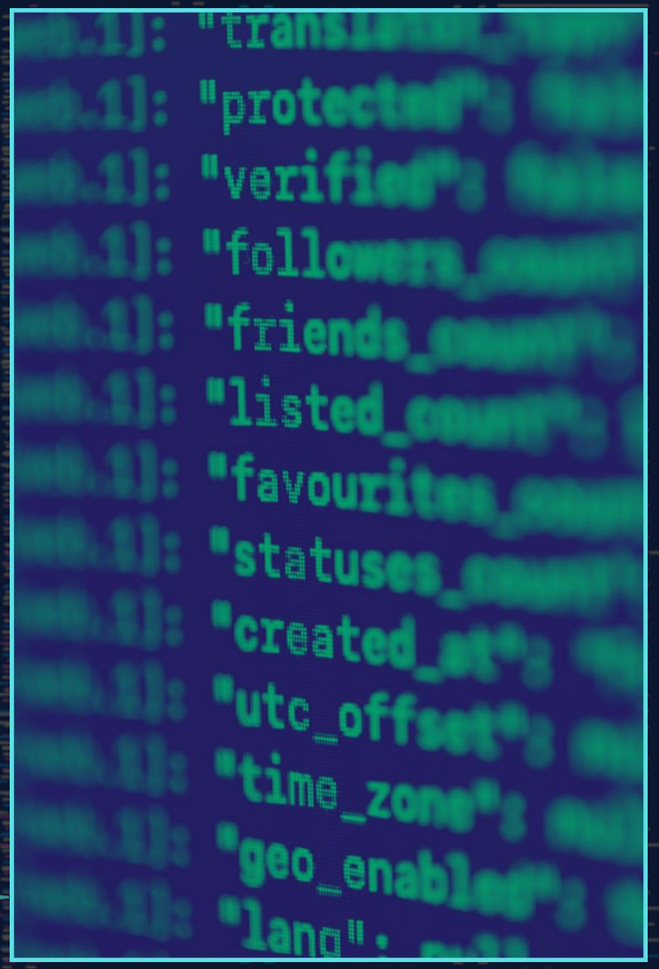
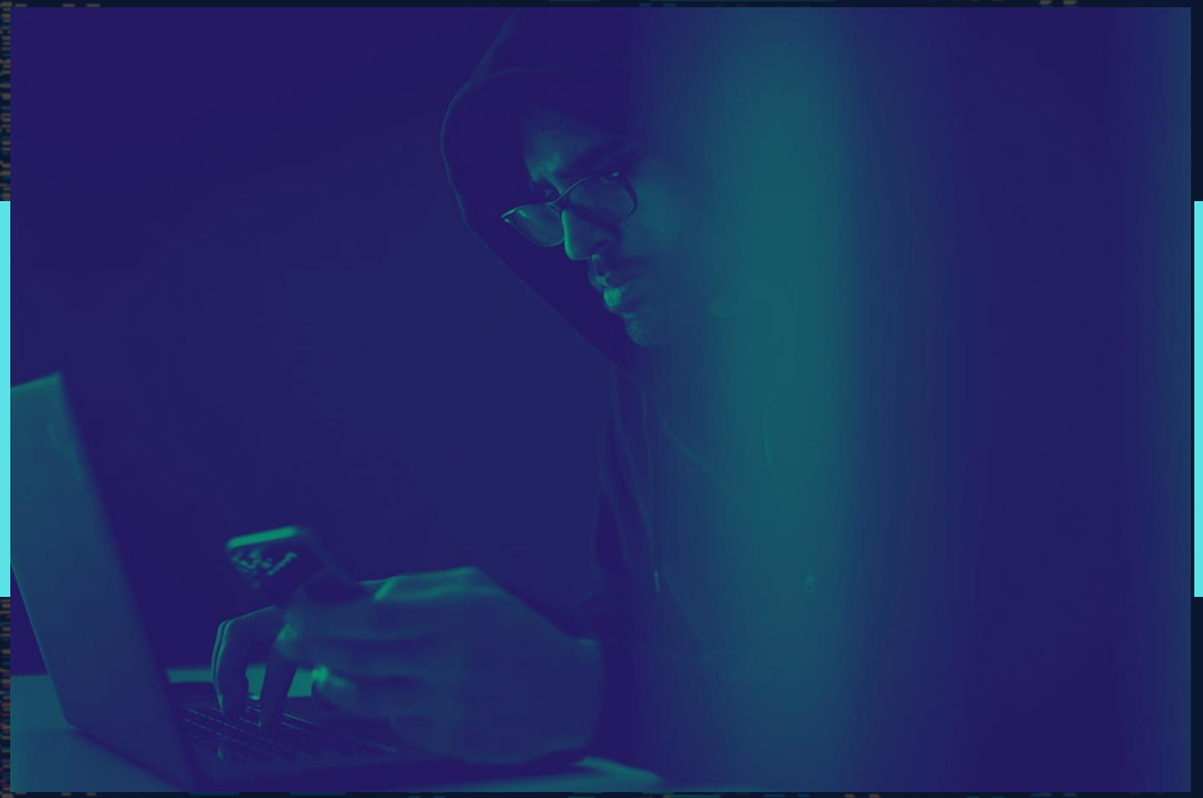
Más allá de las firmas: ¿Cómo funcionan los sistemas antimalware?

Martina Lopez & Mario Micucci

Security Researchers @ ESET

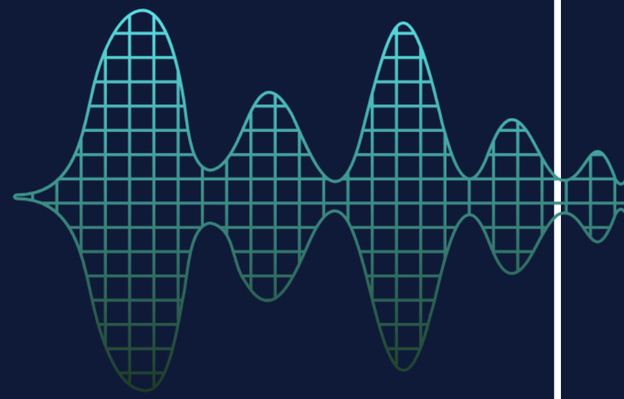




¡Bienvenidos/as!

¿Quiénes somos? ¿Qué hacemos acá? ¿Alguno/a usa antivirus? ¿Qué gusto tiene la sal?

ls charla/



01.

INTRODUCCION HISTÓRICA

02.

TÉCNICAS Y DESAFÍOS

03.

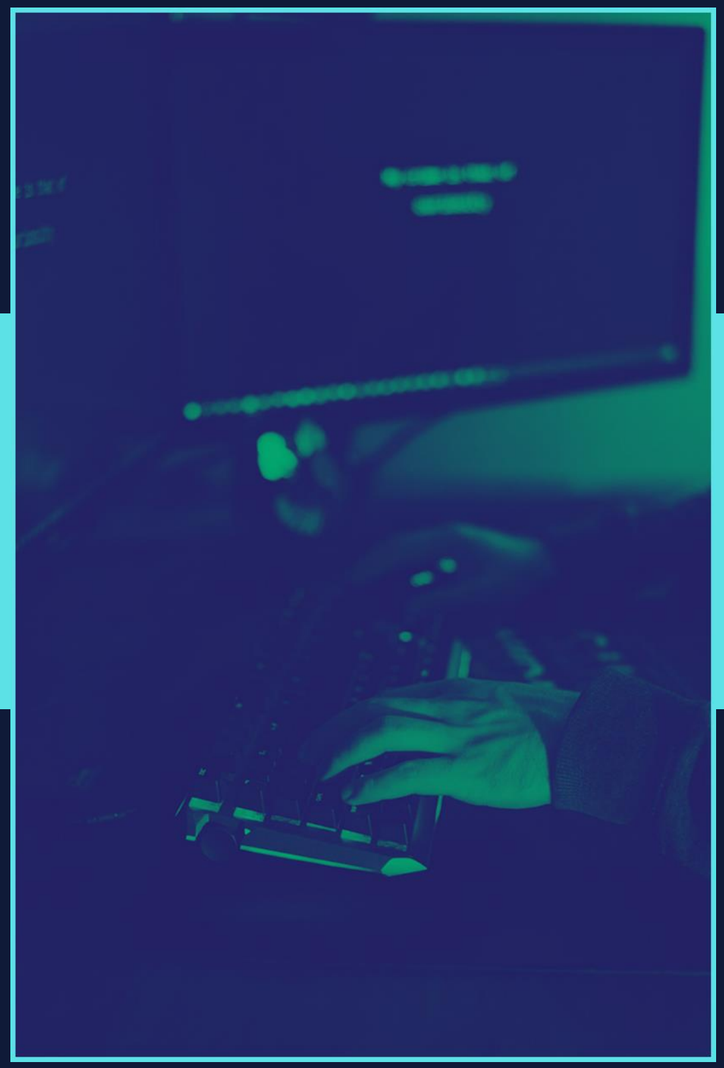
IA Y EL FUTURO

01. INTRODUCCIÓN

En los albores de la era digital, cuando los arcanos del ciberespacio recién se descubrían, surgieron las primeras huestes del mal.

Ante tan funestos augurios, los primeros sabios forjaron talismanes de defensa, los antivirus, herramientas sencillas basadas en las firmaturas del enemigo.

Mas no tardó en llegar el día en que el malware, taimado y cambiante, escapó de sus cadenas primitivas, forzando a los guardianes a templar armas más complejas y sutiles.



UN REPASO HISTÓRICO

1980

Virus en disquetes

Avs basados en firmas

1990

Malware polimórfico

Heurísticas rudimentarias

2000

Ransomware, ocultamiento

Sandboxing

2010

Ataques dirigidos

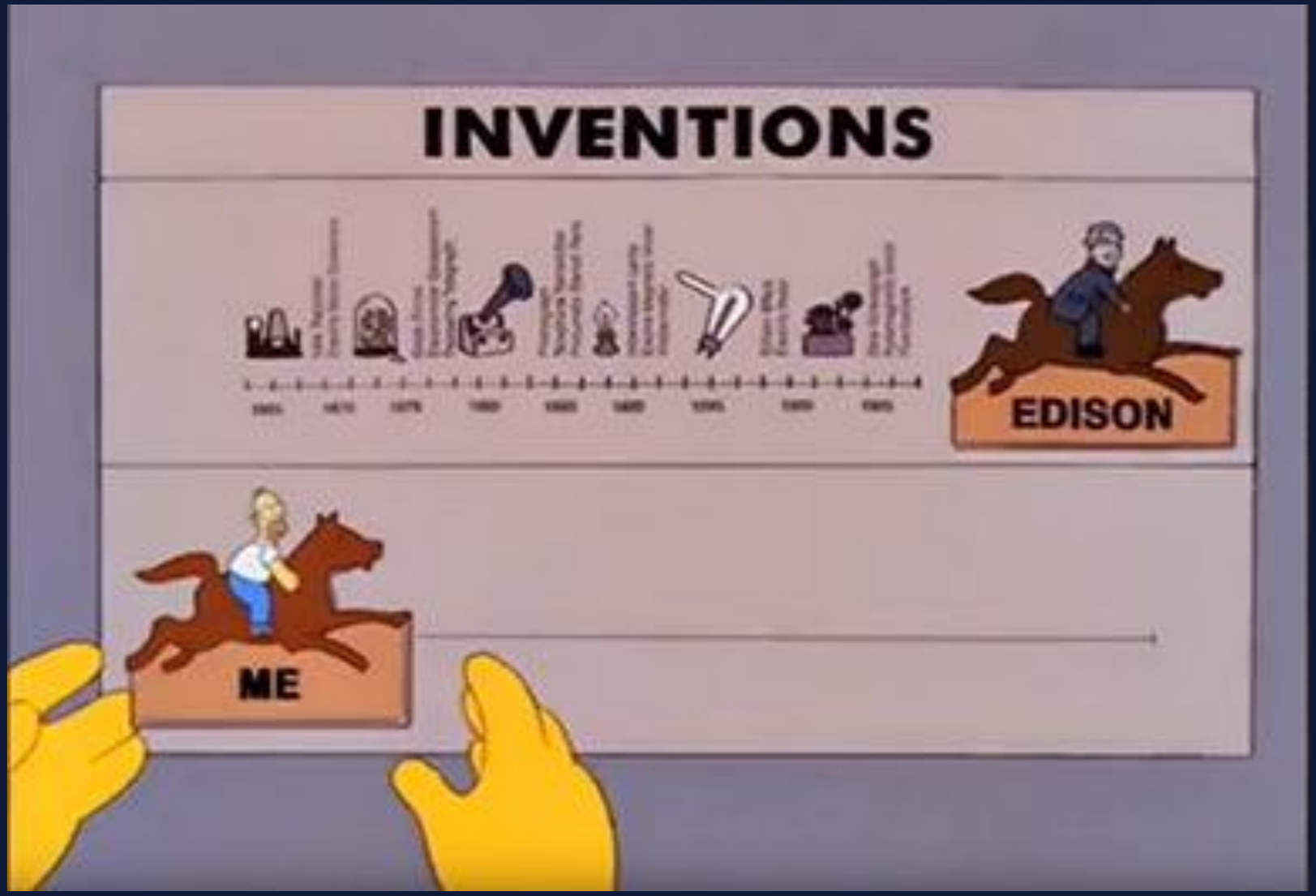
Monitoreo de red

2020

IA y automatización (ataque)

IA y automatización (defensa)

UN REPASO HISTÓRICO



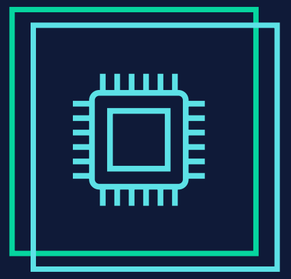
02. TÉCNICAS Y DESAFÍOS

En esta eterna pugna entre el bien y el mal, los sabios antimalware han desarrollado artes finas de detección, métodos variados como la heurística y la vigilancia de patrones.

Empero, el enemigo, astuto como zorro en la noche, adopta formas cambiantes: el polimorfismo y el metamorfismo, estratagemas que le permiten esconder su verdadera faz y burlar las miradas de los guardianes.

Los sistemas, cual vigías incansables, escrutan las sombras en busca de movimientos sospechosos.,

MODULARIDAD

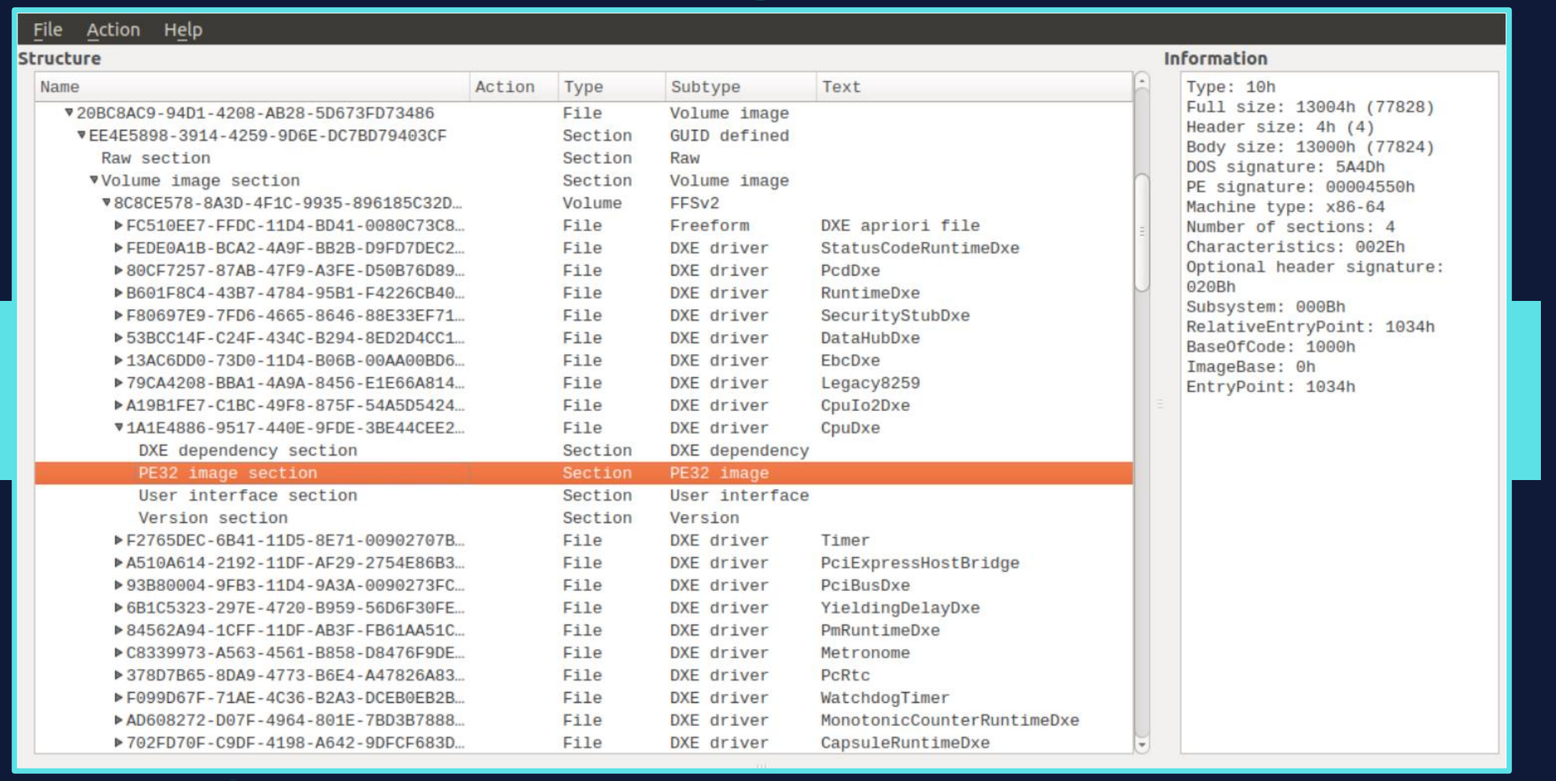


UEFI

ADN

MEMORIA

UEFI: El código antes del código



M I L F

M

MONITOREO DE INTEGRIDAD

del firmware, comparando con una imagen o hash limpio

I

INVESTIGACIÓN DE COMPORTAMIENTO

buscando acciones inusuales o potencialmente riesgosas

L

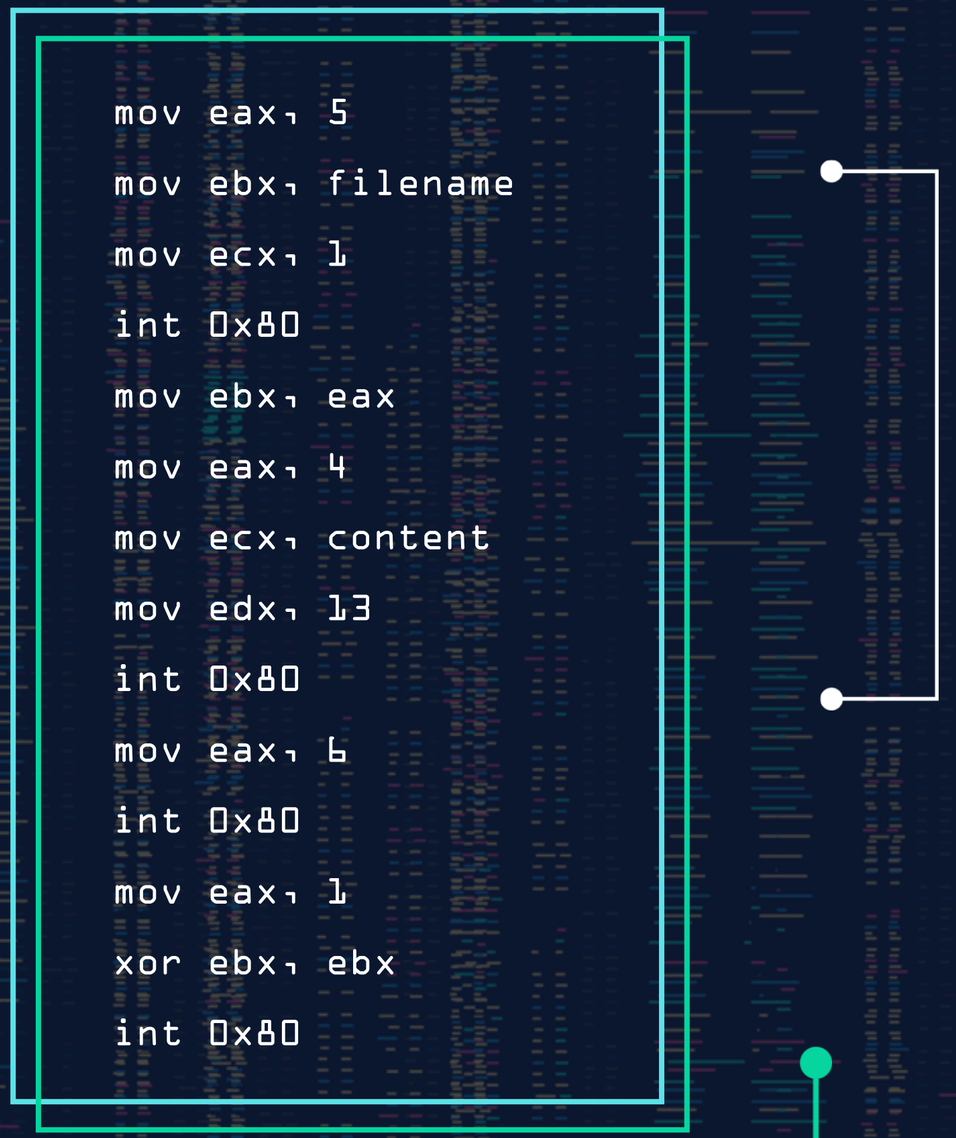
LECTURA Y DESENSAMBLADO

detectando manipulaciones en el flujo de arranque

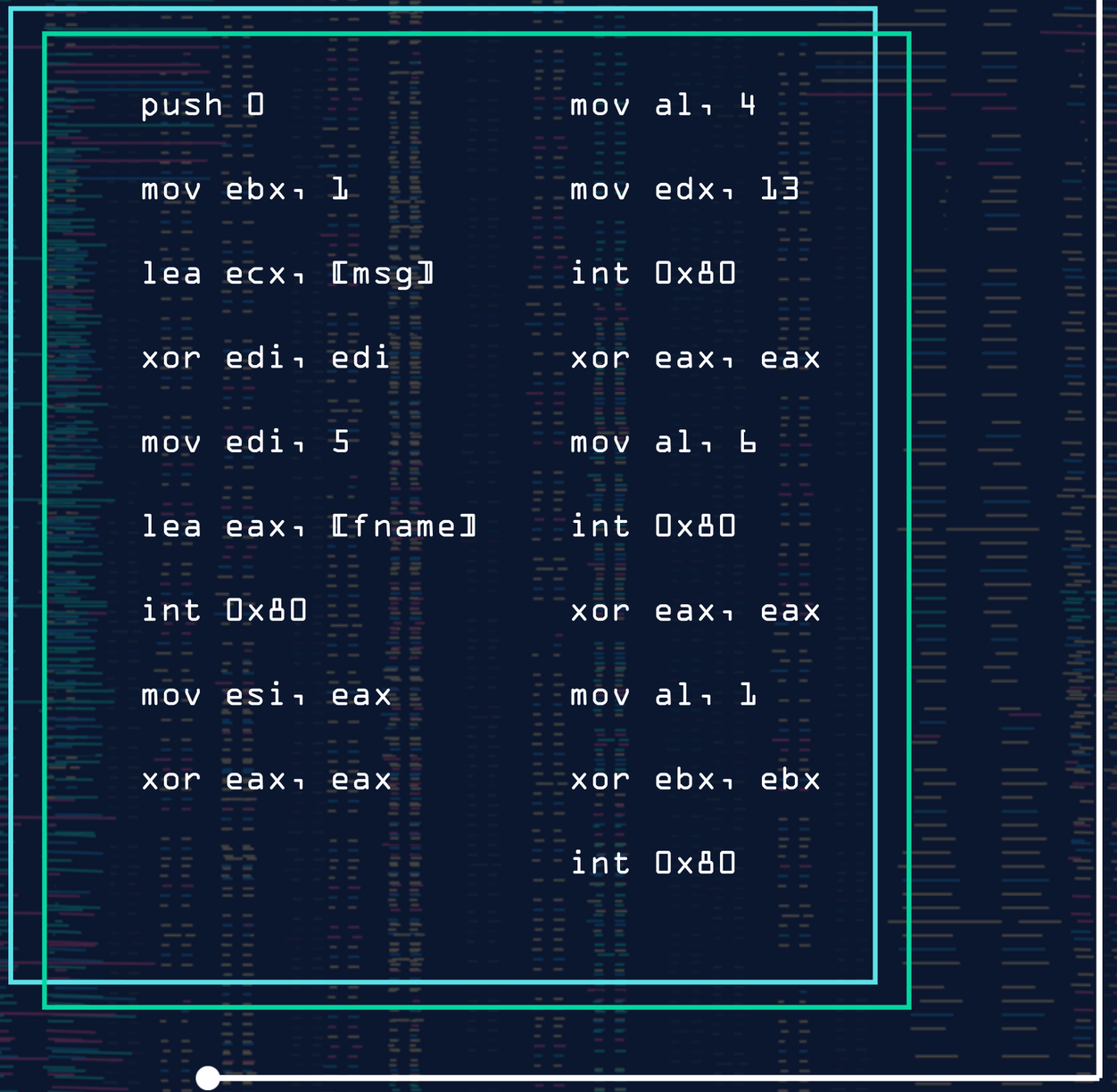
F

FILTRADO Y MITIGACIÓN

bloqueando amenazas o deteniendo el arranque



```
mov eax, 5
mov ebx, filename
mov ecx, 1
int 0x80
mov ebx, eax
mov eax, 4
mov ecx, content
mov edx, 13
int 0x80
mov eax, 6
int 0x80
mov eax, 1
xor ebx, ebx
int 0x80
```



```
push 0
mov ebx, 1
lea ecx, [msg]
xor edi, edi
mov edi, 5
lea eax, [fname]
int 0x80
mov esi, eax
xor eax, eax
mov al, 4
mov edx, 13
int 0x80
xor eax, eax
mov al, 6
int 0x80
xor eax, eax
mov al, 1
xor ebx, ebx
int 0x80
```

Comienza la ejecución

Abre un archivo

Escribe un mensaje

Finaliza la ejecución

ADN

Comienza la ejecución

Realiza acciones temporales

Abre un archivo

Escribe un mensaje

Realiza acciones temporales

Finaliza la ejecución

¿POR QUE NOS INTERESA LA MEMORIA?

Fileless

Payload en memoria

Obfuscado

Payload en secuencia

Inyección de código

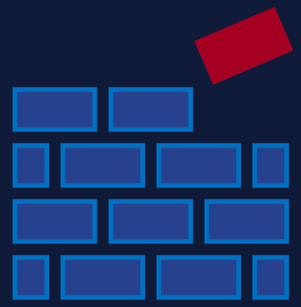
Modo kernel

Polimorfismo

¿QUÉ BUSCAMOS?

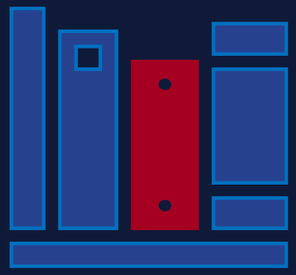
LLAMADAS AL SISTEMA

catalogadas como
“críticas” o “alarmantes



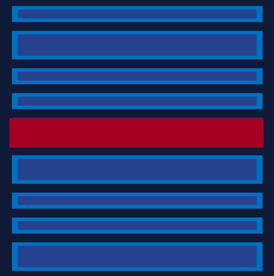
CARGA DE BIBLIOTECAS

o cualquier indicio de un
cambio en tiempo de ejecución



PAGINAS DE MEMORIA

ejecutables, solicitadas o
modificadas recientemente



HEAP Y STACK

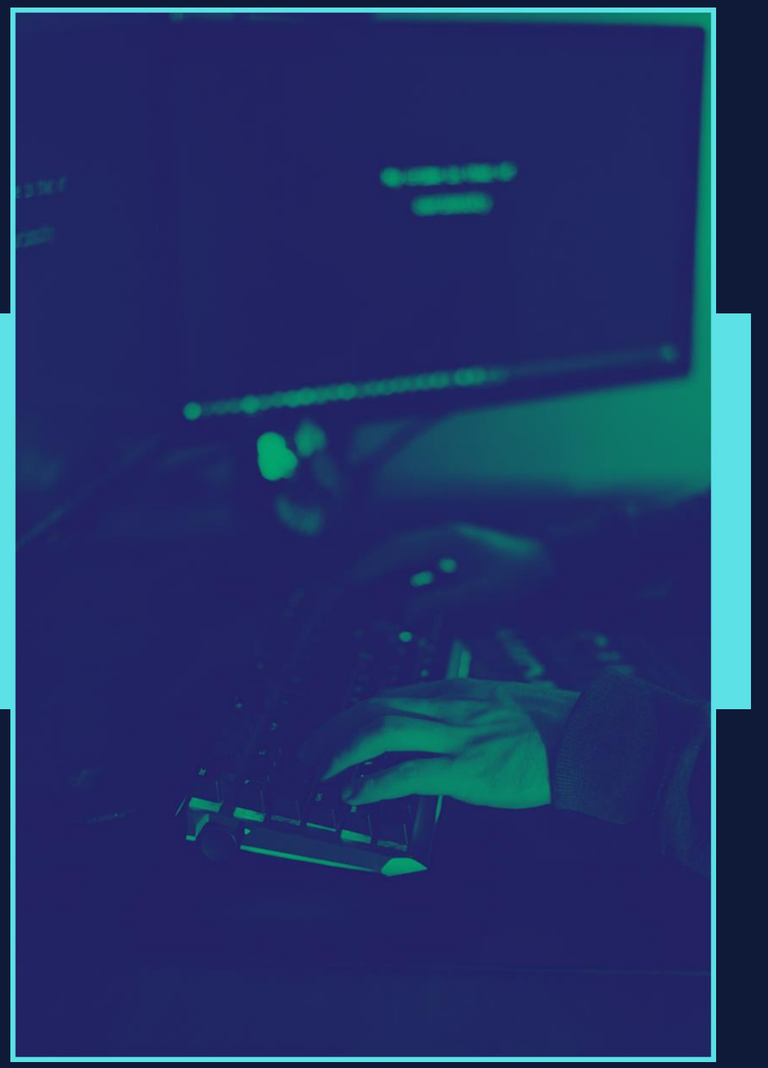
manipulaciones o
sobreescrituras recientes

03. IA Y EL FUTURO

Y he aquí que la ciencia arcana de la inteligencia artificial se une a los protectores, pues es tal su poder que no sólo contempla lo presente, sino que, cual oráculo, augura lo venidero.

Gracias a sus artes, los antimalware pueden prever las amenazas futuras y ajustar sus escudos y lanzas a lo inesperado.

Mas, como toda magia, la IA también conlleva sus propios retos: desde los falsos avisos hasta la demanda de vastos recursos, plantea dilemas que deben tratarse con prudencia y sabiduría.



Las bondades de la IA

Anális Predictivo

Automatización y Velocidad de Respuesta

Análisis de Comportamiento

Reducción de Falsos Positivos


NO TODO LO QUE
BRILLA ES ORO

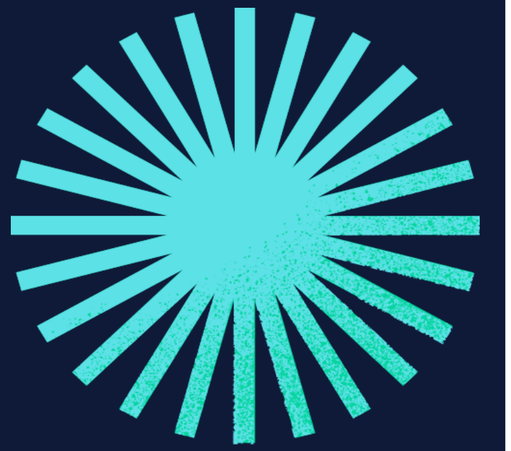
Desafíos de la IA

Falsos Positivos y Negativos

Consumo de Recursos

Dependencia de Datos de Calidad

Evolución de las Amenazas



Moraleja

01. Cada avance en deteccion provoca una respuesta del adversario

02. La vigilancia y el aprendizaje debe ser constante; En Ciberseguridad descansar es retroceder

03. Debemos enfocarnos en construir una mentalidad resiliente y adaptable, conscientes de que cada defensa nueva invita a un nuevo desafío, y que la seguridad no es un destino, sino un viaje sin final.

TL;DR

VACUNATE ANTES DE QUE TE VACUNEN