
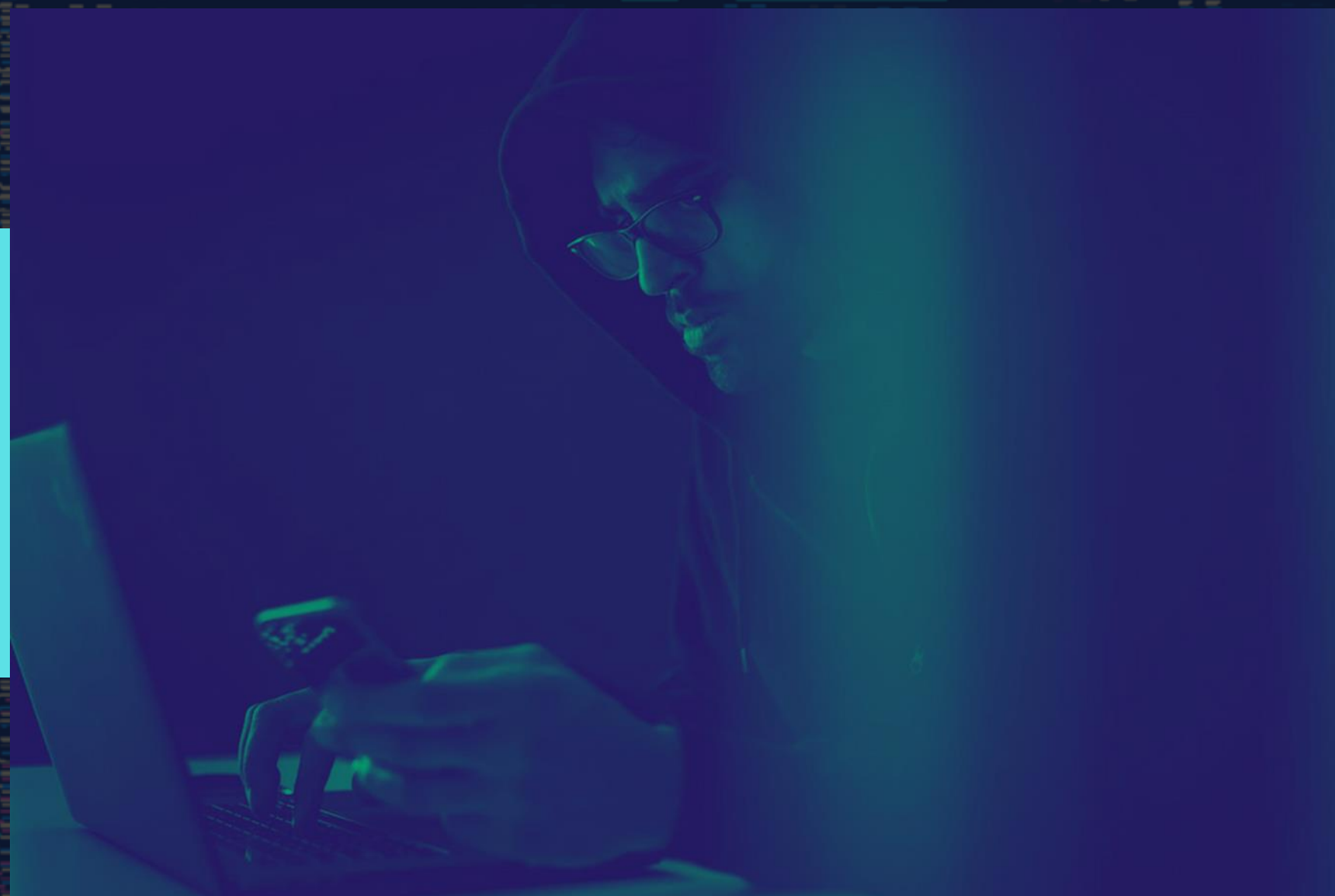


Más allá de las firmas: ¿Cómo funcionan los sistemas antimalware?

Martina Lopez & Mario Micucci
Security Researchers @ ESET



```
obj.1): "translator": null
obj.1): "protector": null
obj.1): "verifier": null
obj.1): "followers_count": 0
obj.1): "friends_count": 0
obj.1): "listed_count": 0
obj.1): "favourites_count": 0
obj.1): "statuses_count": 0
obj.1): "created_at": "2013-04-15T13:27:00Z"
obj.1): "utc_offset": -5
obj.1): "time_zone": "America/Buenos_Aires"
obj.1): "geo_enabled": true
obj.1): "lang": "es"
```

¡Bienvenidos/as!

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

Is charla/

01.

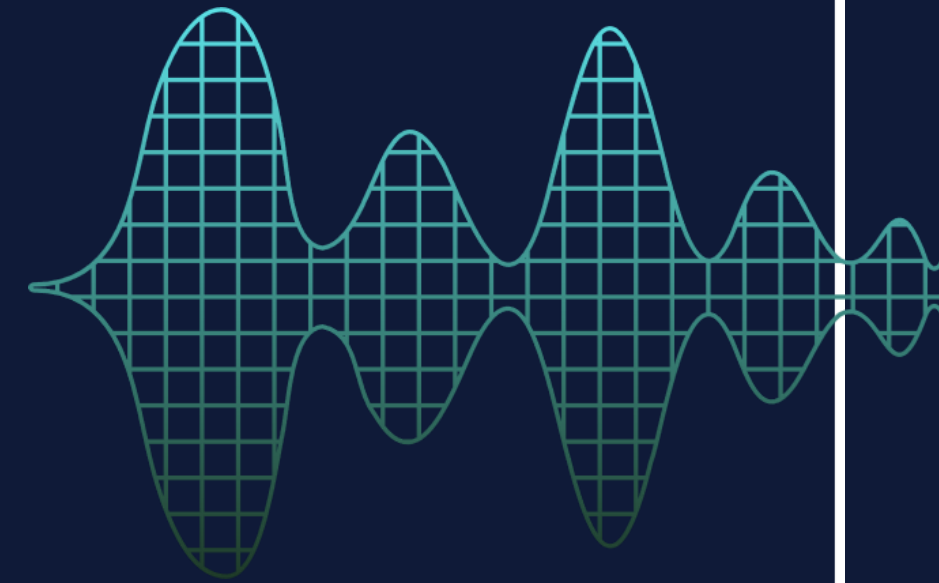
INTRODUCCION
HISTÓRICA

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 temprar armas más complejas y sutiles.



UN REPASO HISTÓRICO

1980

Virus en disquetes
Avs basados en firmas

Malware polimórfico
Heurísticas rudimentarias

1990

Ataques dirigidos
Monitoreo de red

2000

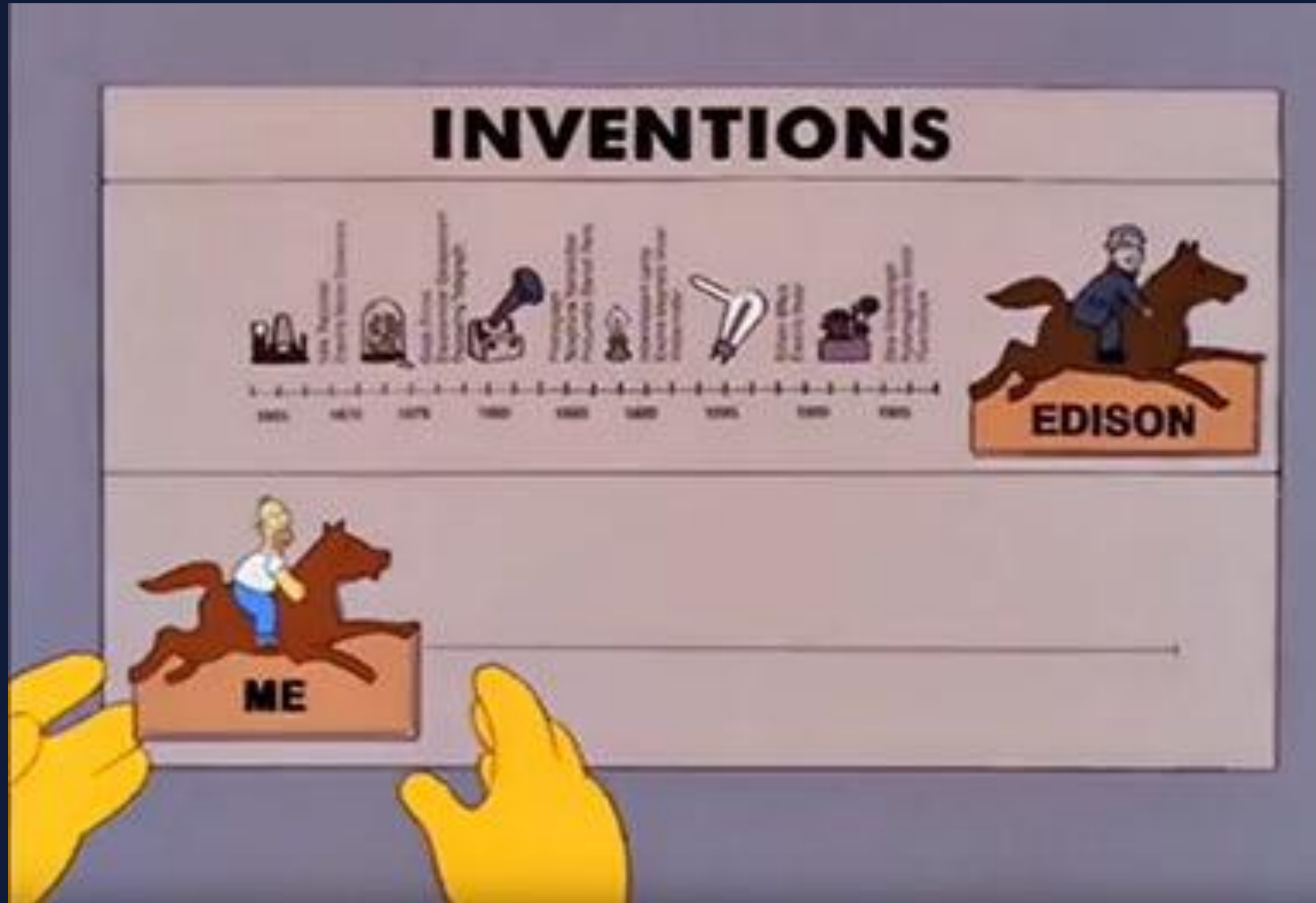
Ransomware, ocultamiento
Sandboxing

2010

2020

IA y automatización (ataque)
IA y automatización (defensa)

UN REPASO HISTÓRICO



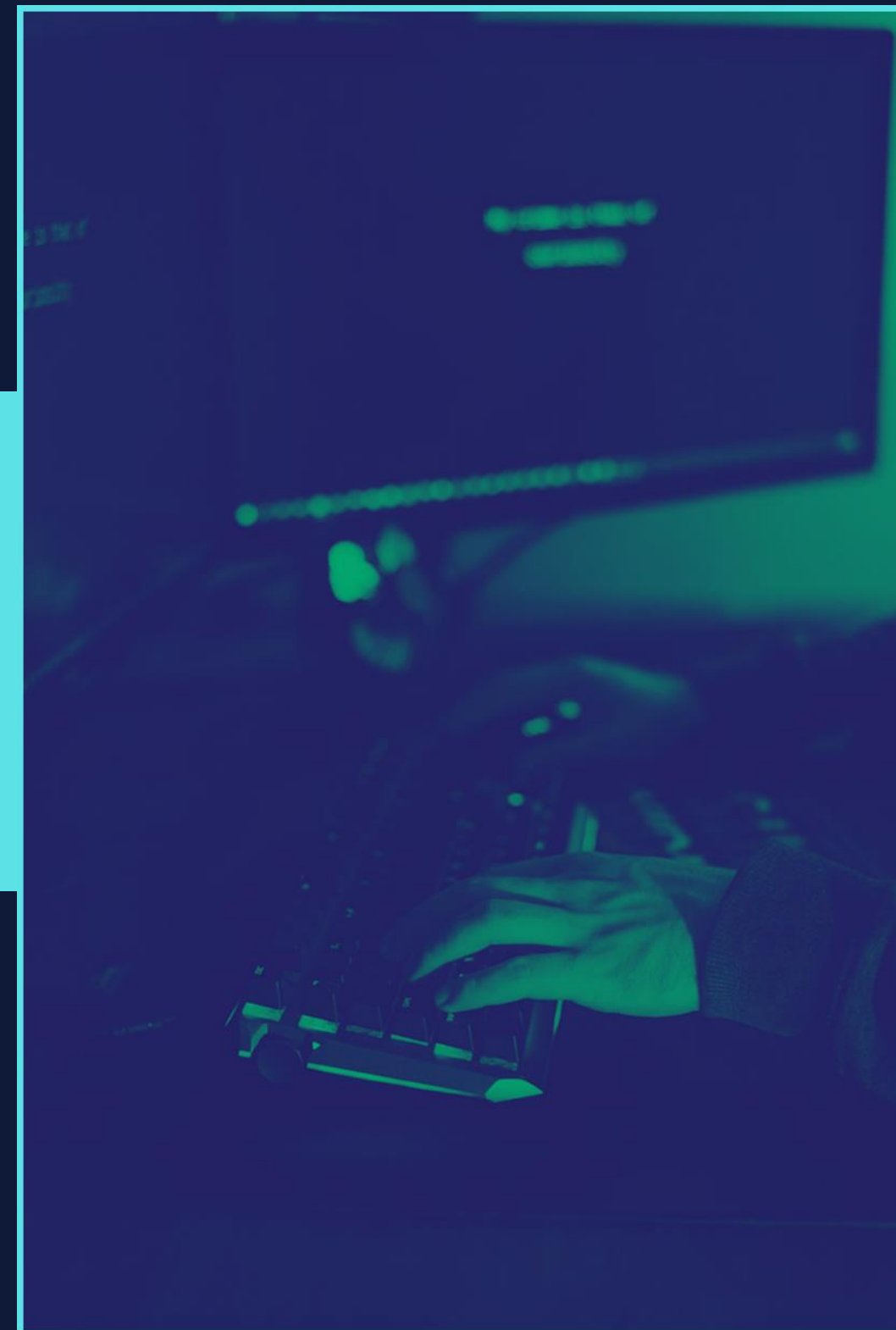
02.

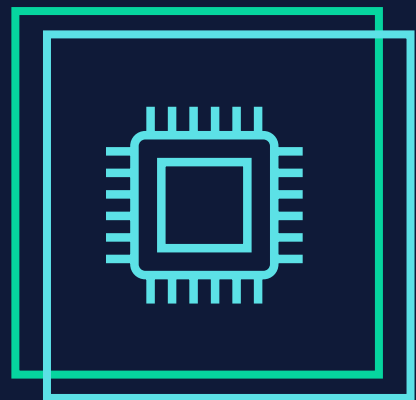
TÉCNICAS Y DESAFÍOS

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, estrategias 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.,

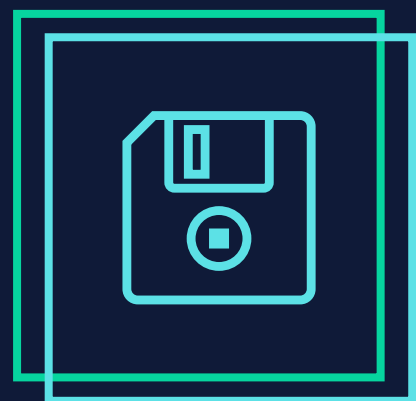




UEFI



ADN



MEMORIA

MODULARIDAD

UEFI: El código antes del código



File Action Help

Structure

Name	Action	Type	Subtype	Text
▼ 20BC8AC9-94D1-4208-AB28-5D673FD73486		File	Volume image	
▼ EE4E5898-3914-4259-9D6E-DC7BD79403CF		Section	GUID defined	
Raw section		Section	Raw	
▼ Volume image section		Section	Volume image	
▼ 8C8CE578-8A3D-4F1C-9935-896185C32D...		Volume	FFSv2	
▶ FC510EE7-FFDC-11D4-BD41-0080C73C8...		File	Freeform	DXE apriori file
▶ FEDE0A1B-BCA2-4A9F-BB2B-D9FD7DEC2...		File	DXE driver	StatusCodeRuntimeDxe
▶ 80CF7257-87AB-47F9-A3FE-D50B76D89...		File	DXE driver	PcdDxe
▶ B601F8C4-43B7-4784-95B1-F4226CB40...		File	DXE driver	RuntimeDxe
▶ F80697E9-7FD6-4665-8646-88E33EF71...		File	DXE driver	SecurityStubDxe
▶ 53BCC14F-C24F-434C-B294-8ED2D4CC1...		File	DXE driver	DataHubDxe
▶ 13AC6DD0-73D0-11D4-B06B-00AA00BD6...		File	DXE driver	EbcDxe
▶ 79CA4208-BBA1-4A9A-8456-E1E66A814...		File	DXE driver	Legacy8259
▶ A19B1FE7-C1BC-49F8-875F-54A5D5424...		File	DXE driver	CpuIo2Dxe
▼ 1A1E4886-9517-440E-9FDE-3BE44CEE2...		File	DXE driver	CpuDxe
DXE dependency section		Section	DXE dependency	
PE32 image section		Section	PE32 image	
User interface section		Section	User interface	
Version section		Section	Version	
▶ F2765DEC-6B41-11D5-8E71-00902707B...		File	DXE driver	Timer
▶ A510A614-2192-11DF-AF29-2754E86B3...		File	DXE driver	PciExpressHostBridge
▶ 93B80004-9FB3-11D4-9A3A-0090273FC...		File	DXE driver	PciBusDxe
▶ 6B1C5323-297E-4720-B959-56D6F30FE...		File	DXE driver	YieldingDelayDxe
▶ 84562A94-1CFF-11DF-AB3F-FB61AA51C...		File	DXE driver	PmRuntimeDxe
▶ C8339973-A563-4561-B858-D8476F9DE...		File	DXE driver	Metronome
▶ 378D7B65-8DA9-4773-B6E4-A47826A83...		File	DXE driver	PcRtc
▶ F099D67F-71AE-4C36-B2A3-DCEB0EB2B...		File	DXE driver	WatchdogTimer
▶ AD608272-D07F-4964-801E-7BD3B7888...		File	DXE driver	MonotonicCounterRuntimeDxe
▶ 702FD70F-C9DF-4198-A642-9DFCF683D...		File	DXE driver	CapsuleRuntimeDxe

Information

Type: 10h
Full size: 13004h (77828)
Header size: 4h (4)
Body size: 13000h (77824)
DOS signature: 5A4Dh
PE signature: 00004550h
Machine type: x86-64
Number of sections: 4
Characteristics: 002Eh
Optional header signature: 020Bh
Subsystem: 000Bh
RelativeEntryPoint: 1034h
BaseOfCode: 1000h
ImageBase: 0h
EntryPoint: 1034h

M

I

L

F



The diagram illustrates the MITL security framework. It consists of four vertical columns, each representing a component of the framework. Each column has a large letter at the top (M, I, L, F) and a descriptive box below it. The letters are white and set against a dark blue background with a cyan border. The descriptive boxes are also dark blue with cyan borders and contain white text. The columns are connected by a series of horizontal and vertical cyan lines, forming a grid-like structure. The background is a dark blue with a pattern of vertical lines in various colors (cyan, red, blue) and a grid of small dots.

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



The image features a dark blue background with a faint, colorful digital rain pattern. Two rectangular blocks of assembly code are highlighted with cyan borders. White lines with circular endpoints connect the blocks, indicating a flow or relationship. The first block on the left contains 13 lines of assembly code. The second block on the right contains 16 lines of assembly code, with the first line being a push instruction. The flow lines start from the top of the first block, go up and left, then down and left to the top of the second block. Another flow line starts from the bottom of the first block, goes down and right, then up and right to the bottom of the second block.

```
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

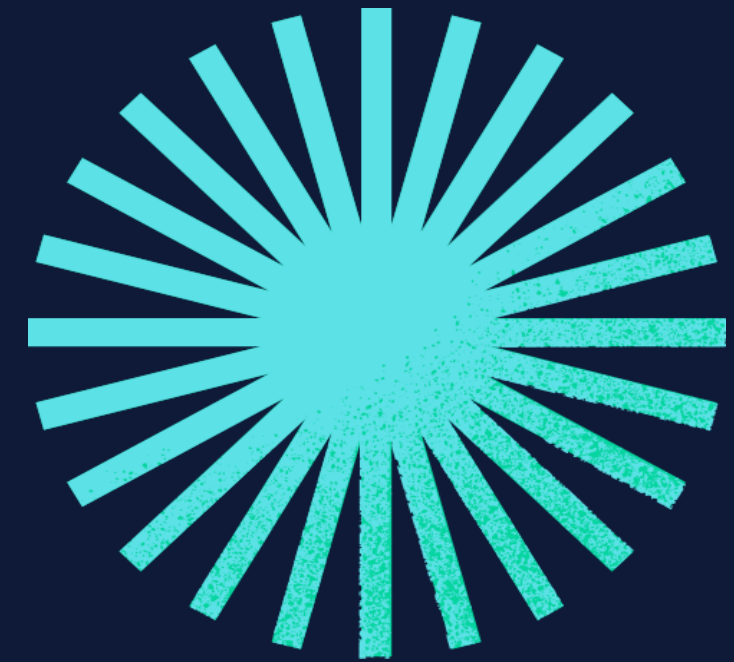
Obfuscado

Payload en secuencia

Inyección de código

Modo kernel

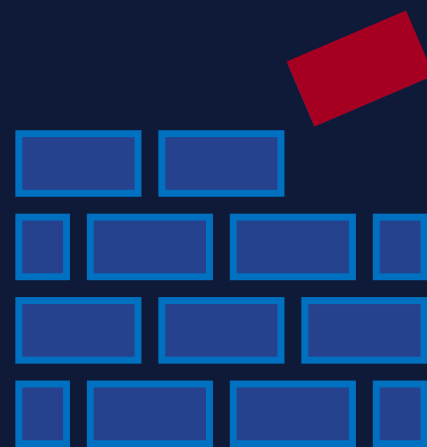
Polimorfismo



¿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
sobreescripciones recientes



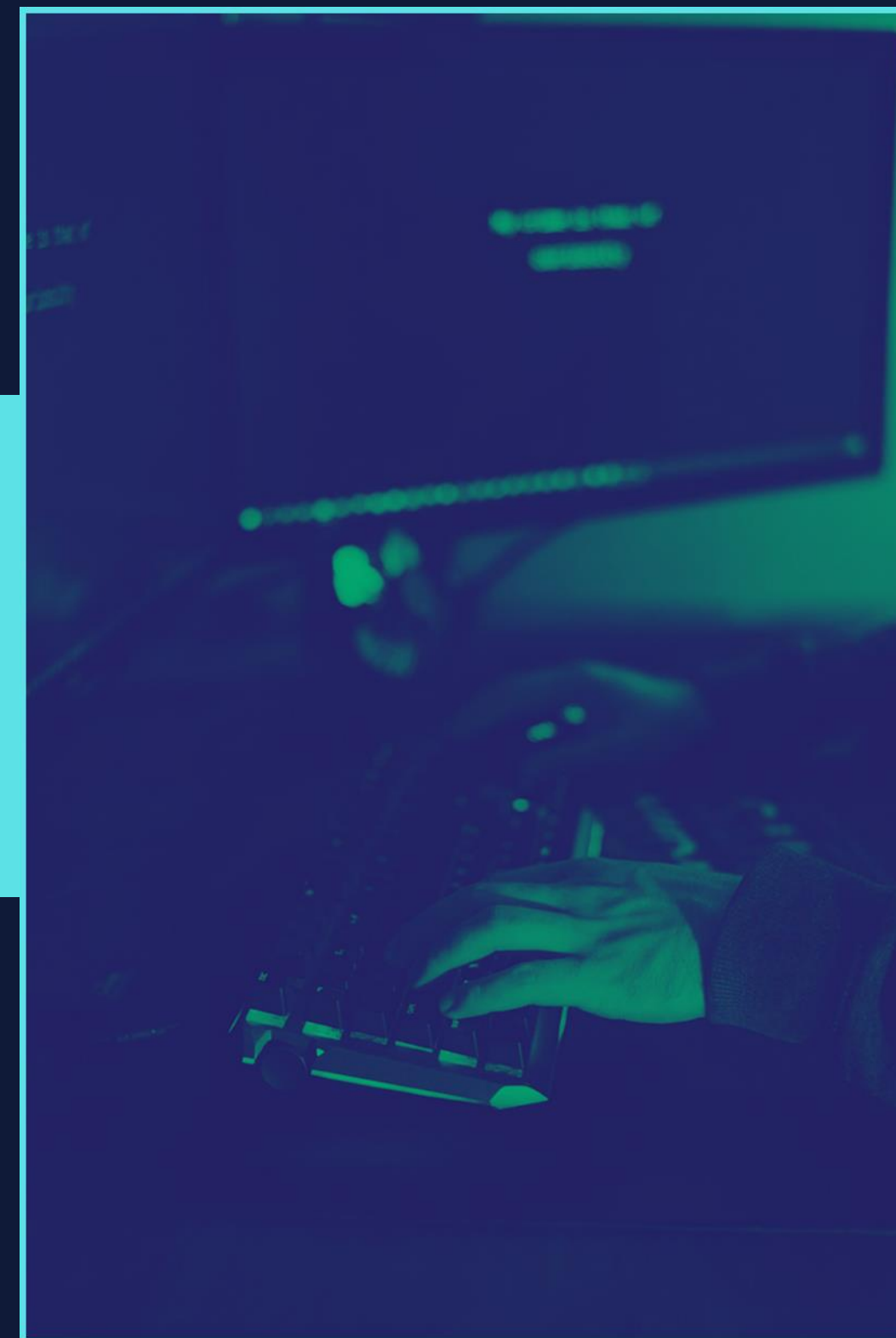
03.

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

Análisis Predictivo

Automatización y Velocidad de Respuesta

Análisis de Comportamiento

Reducción de Falsos Positivos





NO TODO LO QUE
BRILLA ES ORO

BRILLA ES ORO
NO TODO LO QUE

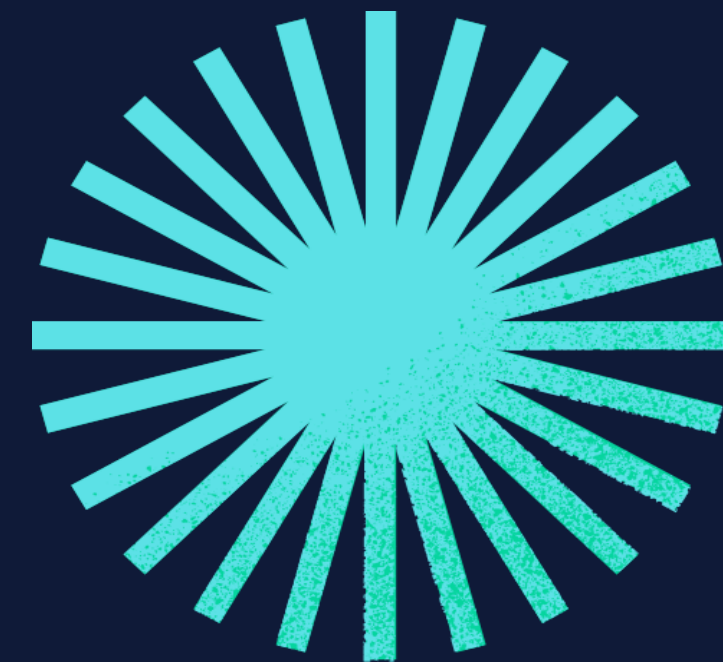
Desafíos de la IA

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 QUETE

VACUNEN

