UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Modulo 1:

Introducción a la Ciberseguridad y Seguridad de la Información

Sesión 1:

Fundamentos de la Ciberseguridad y el Modelo CIA

OBJETIVO DE LA SESIÓN:

Comprender los conceptos esenciales de la ciberseguridad, la importancia de proteger la información y el modelo de seguridad CIA.

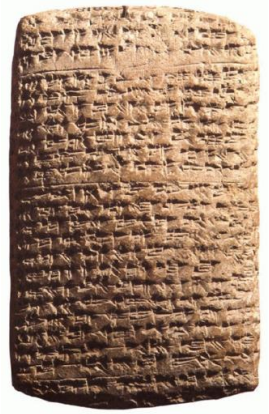
Seguridad de la Información

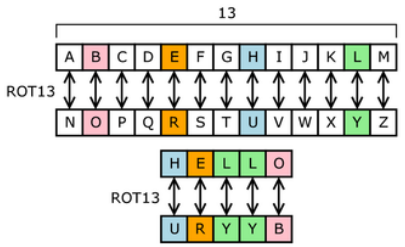
Hoy día es común escuchar preguntas sobre la seguridad de la información: ¿Qué es?, ¿Por qué gobiernos, empresas y personas se preocupan por la seguridad de la información?, ¿Por qué es importante?

Seguridad de la información es el conjunto de conocimientos y técnicas usados para proteger la información y los sistemas de información de accesos, uso, liberación, perturbación, modificación o destrucción no autorizados, con el fin de garantizar tres requerimientos o necesidades fundamentales: confidencialidad, integridad y disponibilidad. (National Institute of Standards, NIST, s.f.)

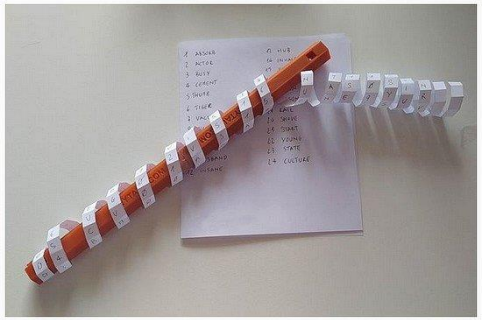
Seguridad de la Información

Mesopotamia
(aprox. 3000 a.C)

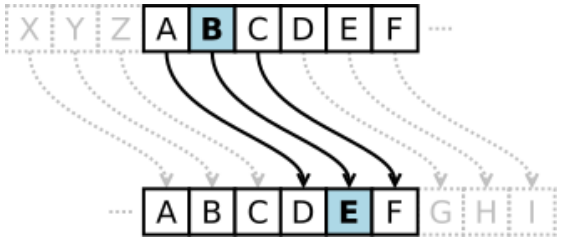


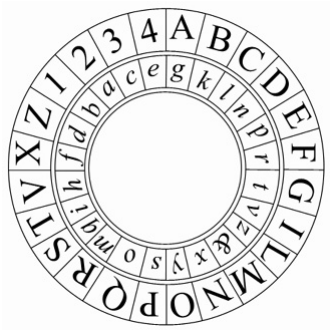


Antigua Grecia
(500-400 a.C)



Cifrado César
(aprox. 58 a.C)



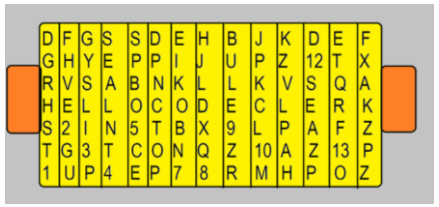


Edad Media
(500-1500 d. C)

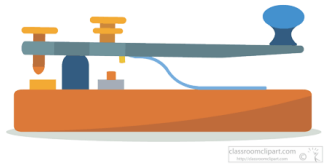
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
05				04		02		01				09					03		08	00					
	19						13			15	14		12			10		17			18			16	
	25	22	21	28								27		23	24	29									26
33						30				39			34				38		36	31			37	32	
					45		41	42			43			49	47			46			48				44
54	52	51	50	53			58					59				55		57		56					
								63			62			61	67		65						64	69	
		78	77				74						73						72		75				
88					85							84		82		81		83		86				87	
		98		91		92		93							90	99	95		97				94		

Seguridad de la Información

Rueda de Jefferson (1795)



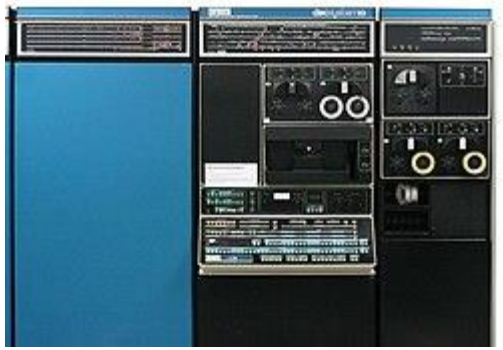
Samuel Morse (1837)

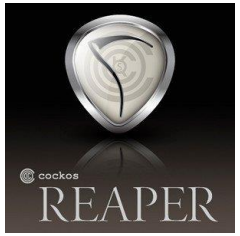


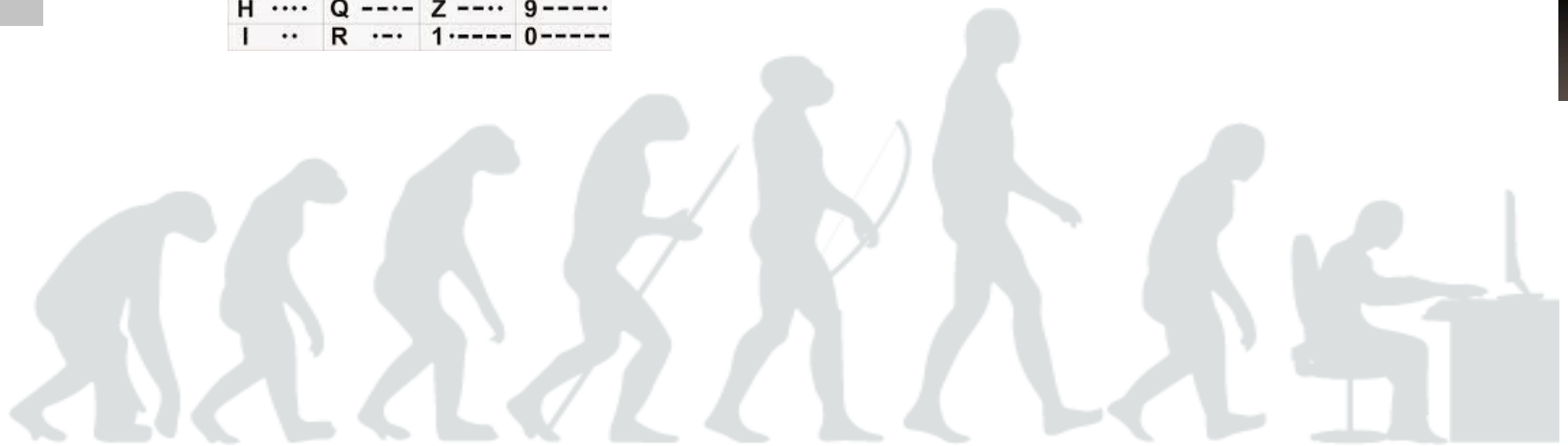
A	·–	J	·–––	S	···	2	··–––
B	–···	K	–·–	T	–	3	···–––
C	–·–·	L	·–··	U	··–	4	····–
D	–··	M	––	V	···–	5	·····
E	·	N	–·	W	·––	6	–····
F	··–·	O	–––	X	–··–	7	––···
G	––·	P	·––·	Y	–·––	8	–––··
H	····	Q	––·–	Z	––··	9	––––·
I	··	R	·–·	1	·––––	0	–––––

Enigma (1918)

Ciberseguridad (1971)







Época	Técnica o Herramienta	Método	Propósito	Ejemplo de uso
Mesopotamia (3000 a.C.)	Escritura cuneiforme	Sustitución	Proteger mensajes	Comunicación secreta entre habitantes
Antigua Grecia (500-400 a.C.)	Escítala	Transposición	Enviar mensajes secretos	Magistrados y militares espartanos
Roma (58 a.C.)	Cifrado César	Sustitución	Proteger comunicaciones militares	Julio César en campañas militares
Edad Media (500-1500 d.C.)	Sustitución homófona	Sustitución	Proteger escritos religiosos	Monjes copistas
1795	Rueda de Jefferson	Mecánico (Sustitución)	Cifrar mensajes secretos	Comunicaciones diplomáticas de EE.UU.
1837	Código Morse	Sustitución	Comunicación rápida (no siempre secreta)	Comunicaciones militares en la Primera Guerra Mundial
Siglo XX (1918-1945)	Máquina Enigma	Mecánico (Sustitución)	Cifrar/descifrar mensajes militares	Fuerzas armadas alemanas en la Segunda Guerra Mundial
Años 70-80	Software antivirus	No criptográfico	Proteger sistemas contra virus	Seguridad de computadoras personales
Años 2000	Seguridad de la información	No criptográfico	Proteger redes corporativas	Empresas frente a ciberataques

Cifrado Cesar

1. Cifrar y descifrar un mensaje usando el Cifrado César.

Paso 1: Elige un mensaje y un desplazamiento:

- Mensaje: SALUDOS
- Desplazamiento: 5

Paso 2: Asigna valores numéricos al alfabeto:

A=0, B=1, C=2, D=3, E=4, F=5, G=6, H=7, I=8, J=9, K=10, L=11, M=12, N=13, O=14, P=15, Q=16, R=17, S=18, T=19, U=20, V=21, W=22, X=23, Y=24, Z=25

Paso 3: Cifra cada letra:

- Suma el desplazamiento (5) al valor numérico de cada letra.
- Si el resultado es mayor o igual a 26, resta 26 (o usa módulo 26: resultado % 26).
- Convierte el nuevo valor numérico a una letra.

SALUDOS:
S (18) → 18 + 5 = 23 → X
A (0) → 0 + 5 = 5 → F
L (11) → 11 + 5 = 16 → Q
U (20) → 20 + 5 = 25 → Z
D (3) → 3 + 5 = 8 → I
O (14) → 14 + 5 = 19 → T
S (18) → 18 + 5 = 23 → X

Mensaje cifrado: XFQZITX

Descifrar el mensaje: HJXFW

H(7) → 7 - 5 = 2 → C
J(9) → 9 - 5 = 4 → E
X(7) → 23 - 5 = 18 → S
F(7) → 5 - 5 = 0 → A
W(7) → 22 - 5 = 17 → R

Mensaje descifrado: CESAR

Actividad práctica

Implementar y experimentar con el Cifrado César en Python.

```
def cifrado_cesar(texto, desplazamiento, cifrar=True):
    resultado = ""
    for char in texto:
        if char.isalpha():
            # Determinar el código ASCII base (mayúsculas o minúsculas)
            ascii_base = ord('A') if char.isupper() else ord('a')
            # Convertir la letra a un número (0-25)
            char_num = ord(char) - ascii_base
            # Aplicar el desplazamiento (cifrar o descifrar)
            if cifrar:
                char_num = (char_num + desplazamiento) % 26
            else:
                char_num = (char_num - desplazamiento) % 26
            # Convertir de nuevo a letra
            resultado += chr(char_num + ascii_base)
        else:
            # Mantener caracteres no alfabéticos sin cambios
            resultado += char
    return resultado
```

Actividad práctica

Descifrar el mensaje en Cifrado Cesar: rxqtghtvjgxsps

```
def descifrar_cesar(mensaje):
    for d in range(1, 26):
        resultado = ""
        for char in mensaje:
            if char.isalpha():
                ascii_base = ord('A') if char.isupper() else ord('a')
                char_num = (ord(char) - ascii_base - d) % 26
                resultado += chr(char_num + ascii_base)
            else:
                resultado += char
        print(f"Desplazamiento {d}: {resultado}")

mensaje = "rxqtghtvjgxsps"
descifrar_cesar (mensaje)
```

Esto es un ataque de **Fuerza Bruta!**

Mensaje descifrado: ciberseguridad

Análisis de Frecuencia

```
def descifrar_cesar_frecuencia(mensaje):
    alfabeto = {'A': 0, 'B': 1, 'C': 2, 'D': 3, 'E': 4, 'F': 5, 'G': 6, 'H': 7, 'I': 8, 'J': 9, 'K': 10, 'L': 11, 'M': 12, 'N': 13, 'O': 14,
                'P': 15, 'Q': 16, 'R': 17, 'S': 18, 'T': 19, 'U': 20, 'V': 21, 'W': 22, 'X': 23, 'Y': 24, 'Z': 25}
    freq = {}
    for char in mensaje.upper():
        if char.isalpha():
            freq[char] = freq.get(char, 0) + 1
    if not freq:
        return
    letra_comun = max(freq, key=freq.get)
    valor_comun = alfabeto[letra_comun]
    letras_objetivo = {'A': 0, 'E': 4,'I': 8, 'O': 14, 'U': 20}
    for letra, valor in letras_objetivo.items():
        d = (valor_comun - valor) % 26
        resultado = ""
        for char in mensaje:
            if char.isalpha():
                ascii_base = ord('A') if char.isupper() else ord('a')
                char_num = (ord(char) - ascii_base - d) % 26
                resultado += chr(char_num + ascii_base)
            else:
                resultado += char
        print(f"Suponiendo '{letra_comun}' es '{letra.lower()}', desplazamiento {d}: {resultado}")
```

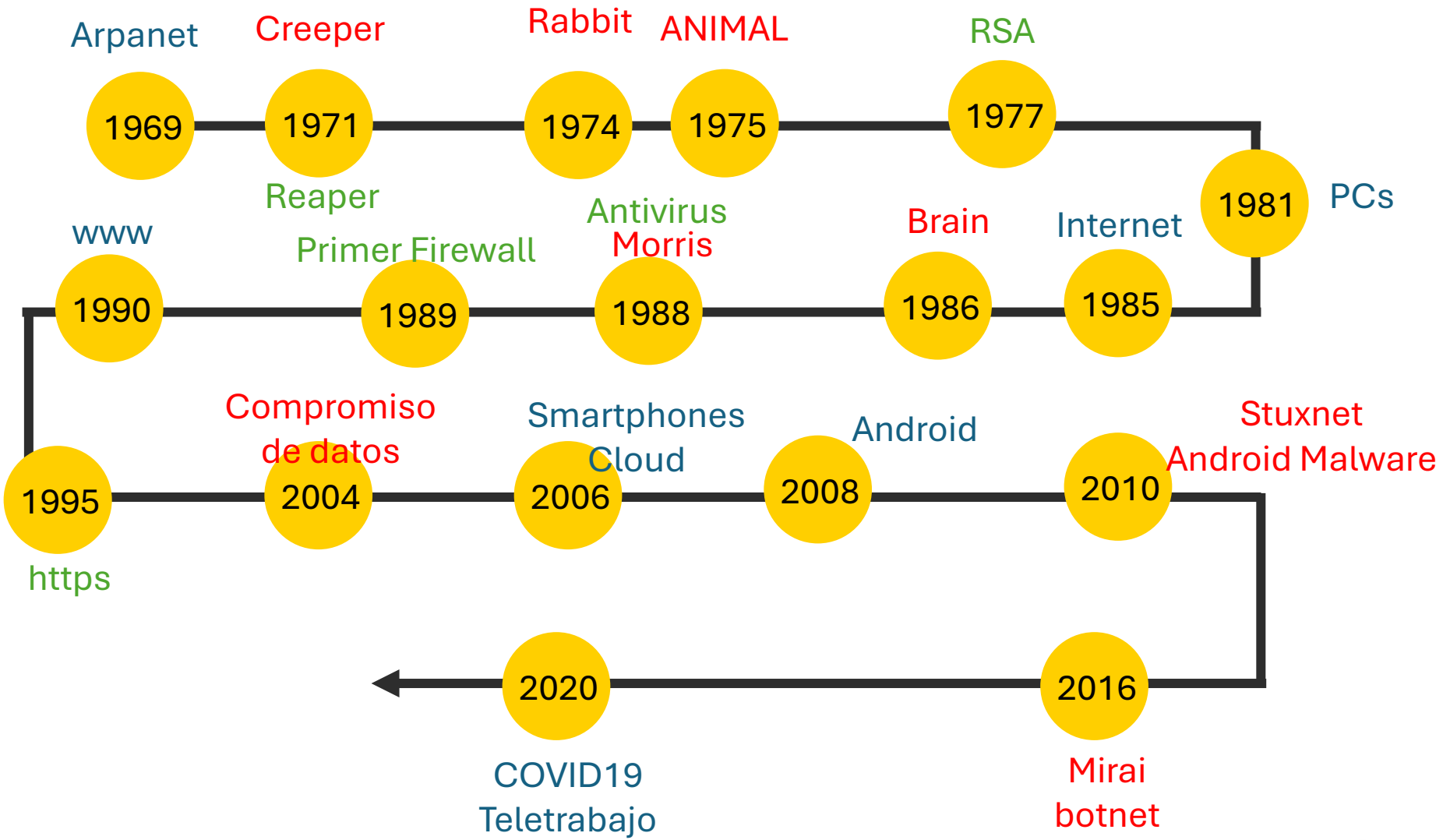
Agregar variabilidad

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
05				04		02		01				09					03		08	00					
	19						13			15	14		12			10		17			18			16	
	25	22	21	28								27		23	24	29									26
33						30				39			34				38		36	31			37	32	
					45		41	42			43			49	47			46			48				44
54	52	51	50	53			58					59				55		57		56					
								63			62			61	67		65						64	69	
		78	77				74						73						72		75				
88					85							84		82		81		83		86				87	
		98		91		92		93							90	99	95		97				94		

¿Qué es la Ciberseguridad?

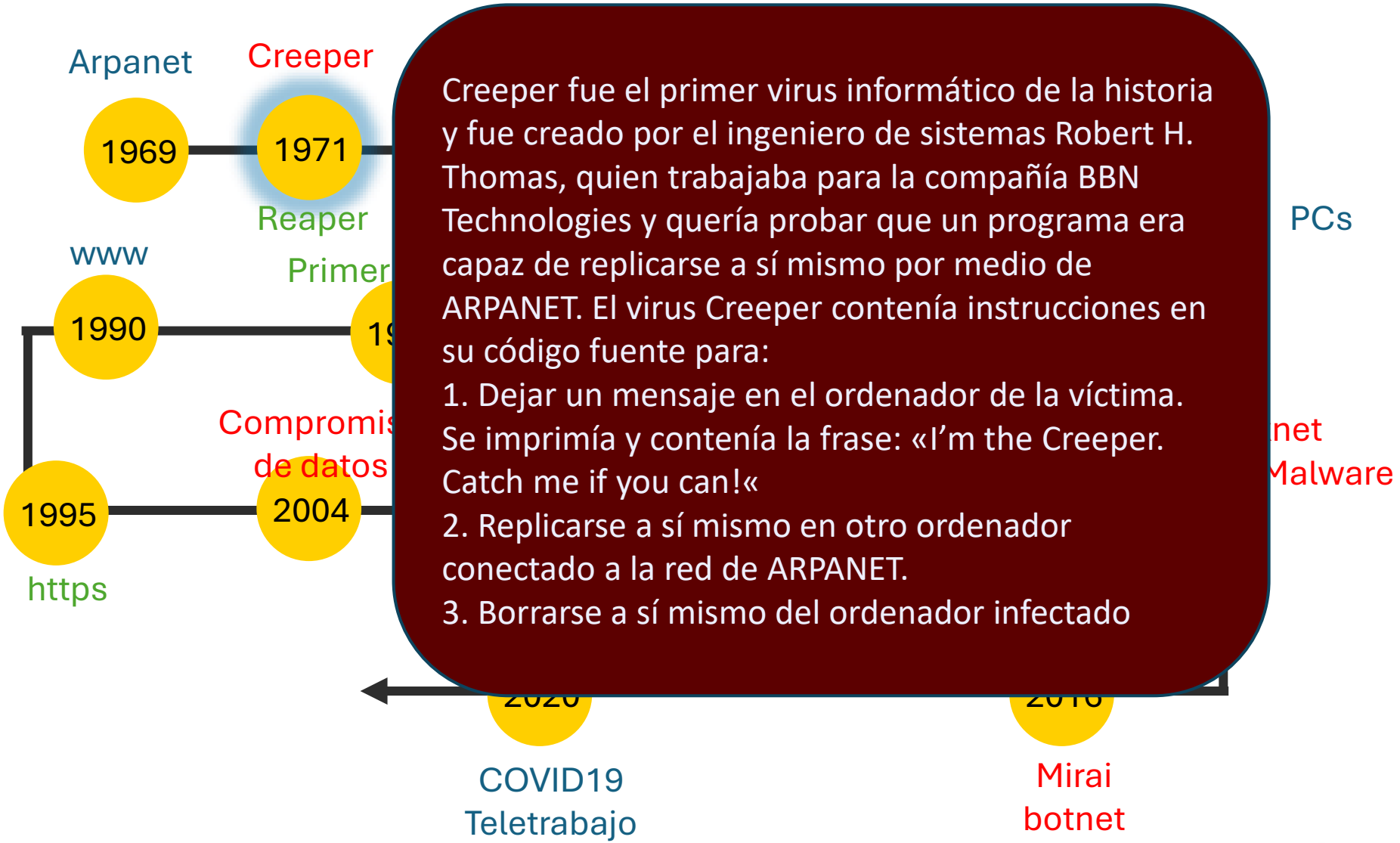
La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales.

Factores sobresalientes en la evolución de la Ciberseguridad



Factores sobresalientes en la evolución de la Ciberseguridad

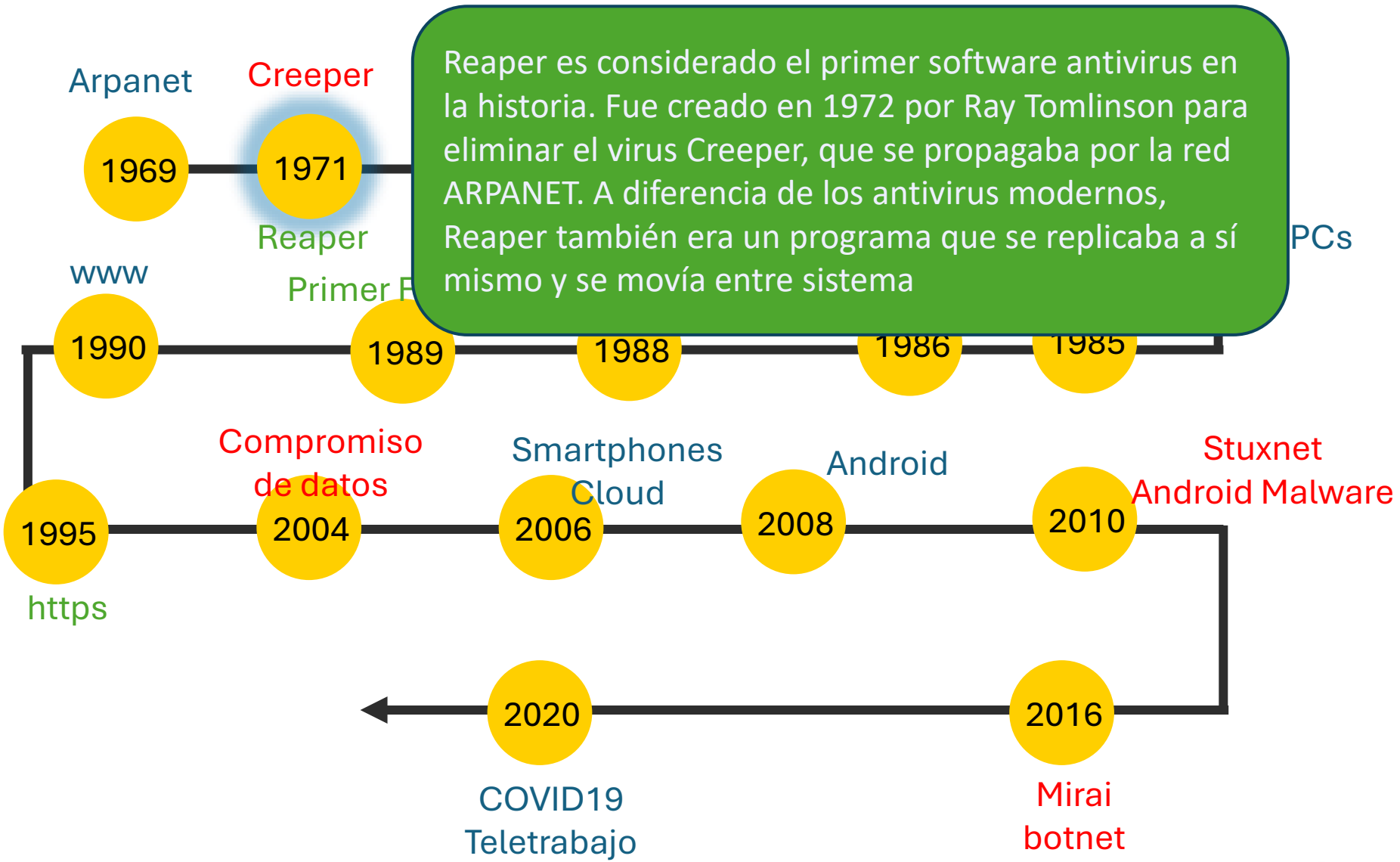
Factores sobresalientes en la evolución de la Ciberseguridad



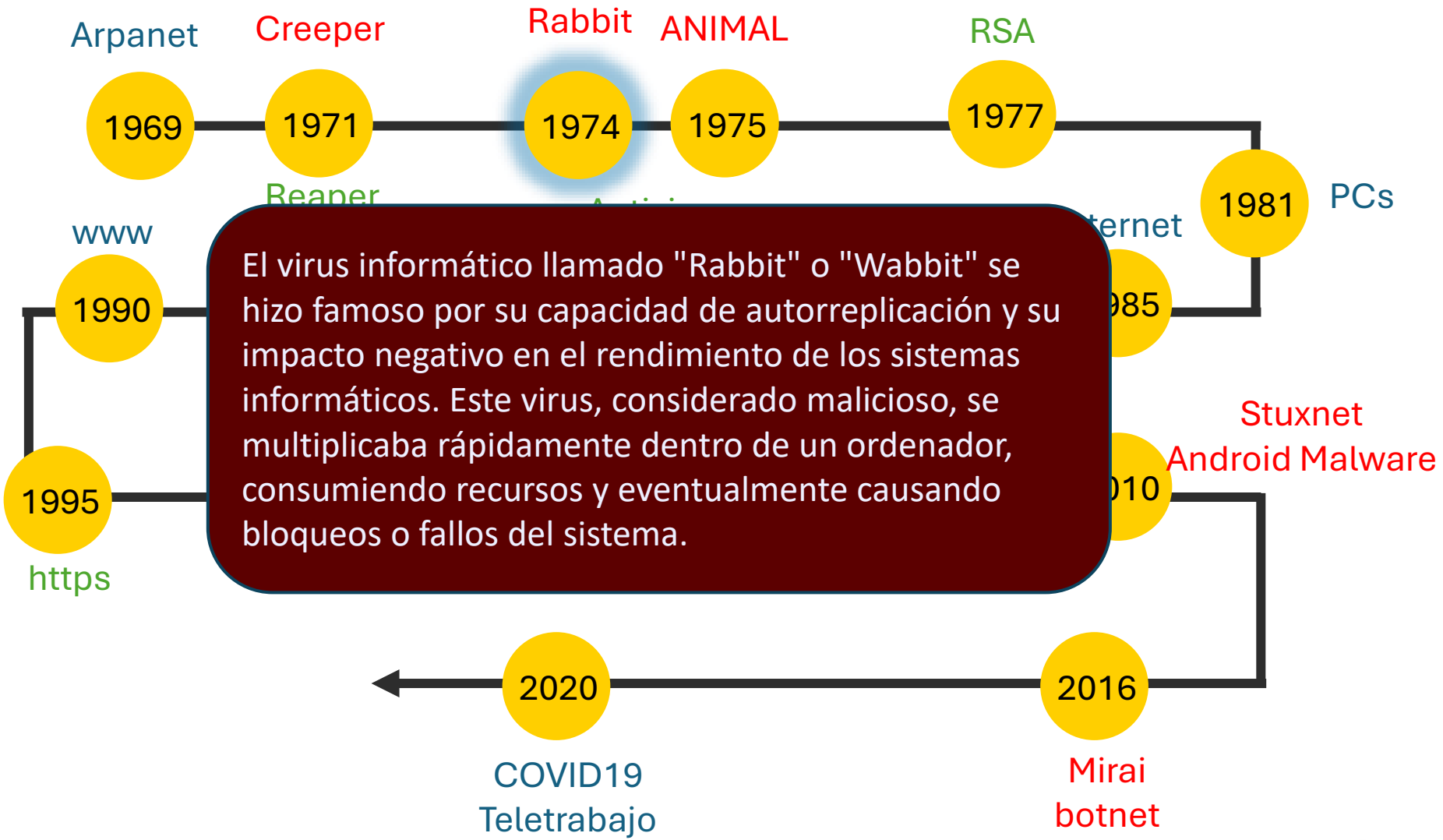
Creeper fue el primer virus informático de la historia y fue creado por el ingeniero de sistemas Robert H. Thomas, quien trabajaba para la compañía BBN Technologies y quería probar que un programa era capaz de replicarse a sí mismo por medio de ARPANET. El virus Creeper contenía instrucciones en su código fuente para:

1. Dejar un mensaje en el ordenador de la víctima. Se imprimía y contenía la frase: «I'm the Creeper. Catch me if you can!«
2. Replicarse a sí mismo en otro ordenador conectado a la red de ARPANET.
3. Borrarse a sí mismo del ordenador infectado

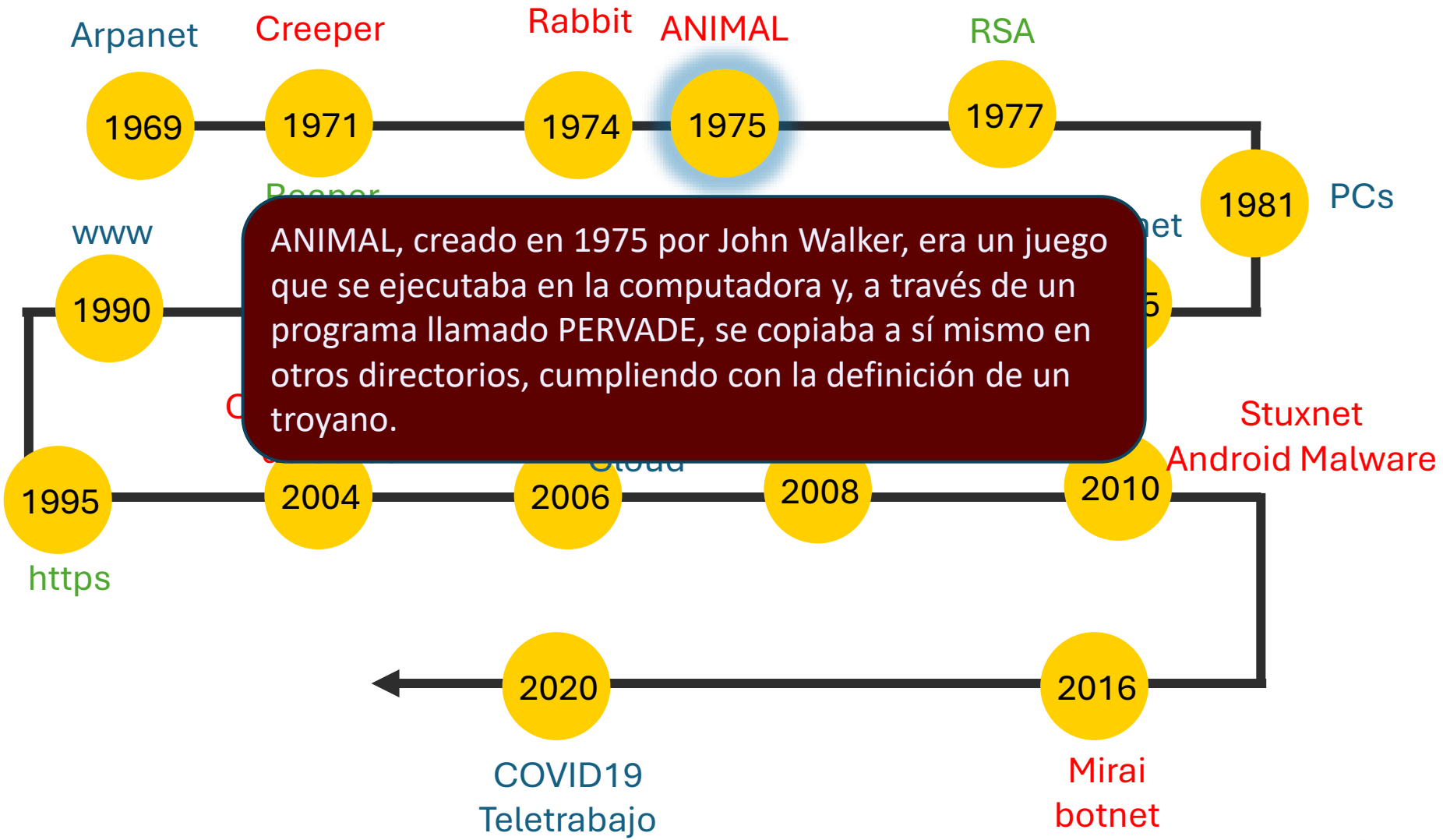
Factores sobresalientes en la evolución de la Ciberseguridad



Factores sobresalientes en la evolución de la Ciberseguridad



Factores sobresalientes en la evolución de la Ciberseguridad

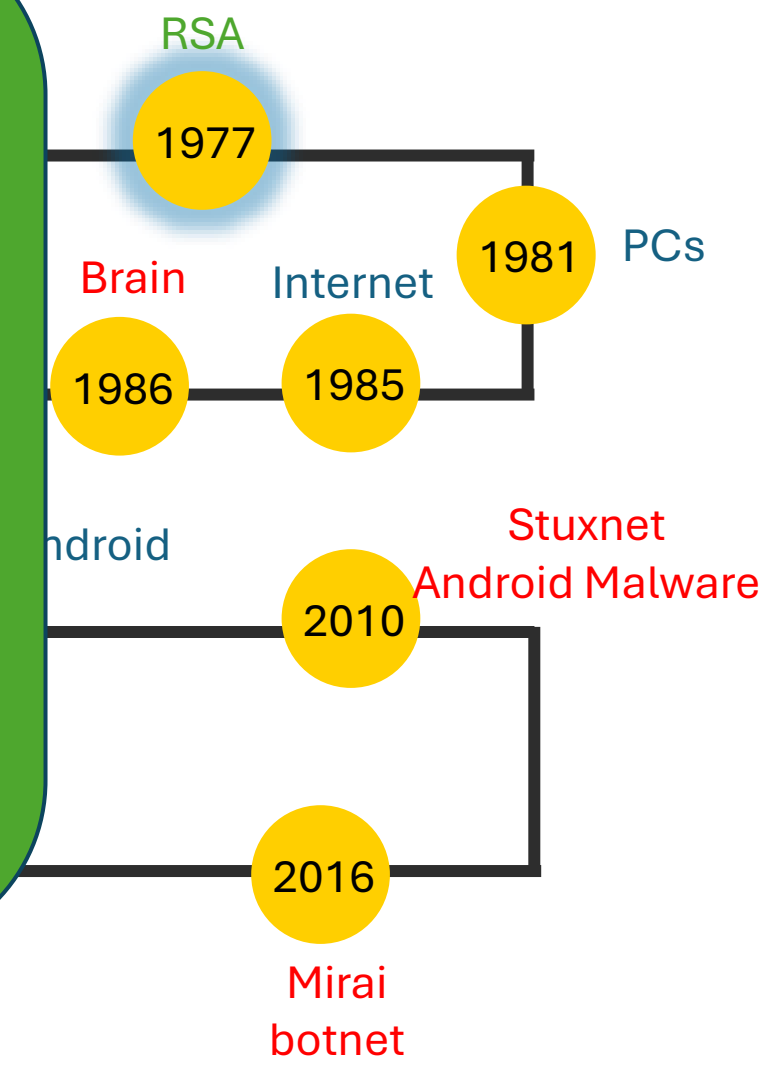


Factores sobresalientes en la evolución de la Ciberseguridad

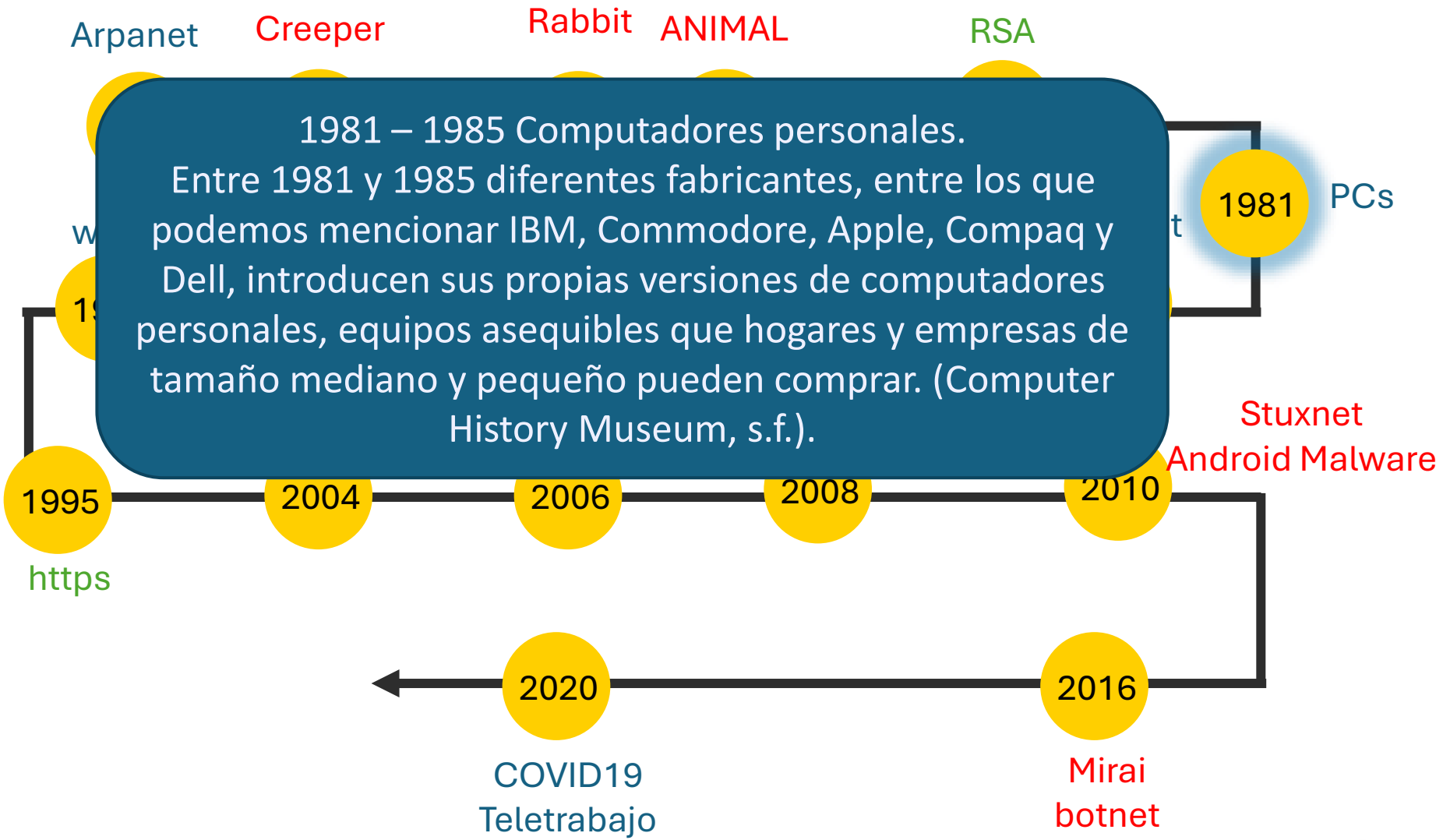
RSA es un algoritmo de criptografía ampliamente utilizado que permite el cifrado y la firma digital. Es un sistema de cifrado asimétrico, lo que significa que utiliza un par de claves: una clave pública para cifrar y una clave privada para descifrar. RSA se basa en la dificultad de factorizar números enteros grandes, lo que hace que sea seguro para la transmisión de datos confidenciales a través de redes inseguras como Internet.

Claves pública y privada:

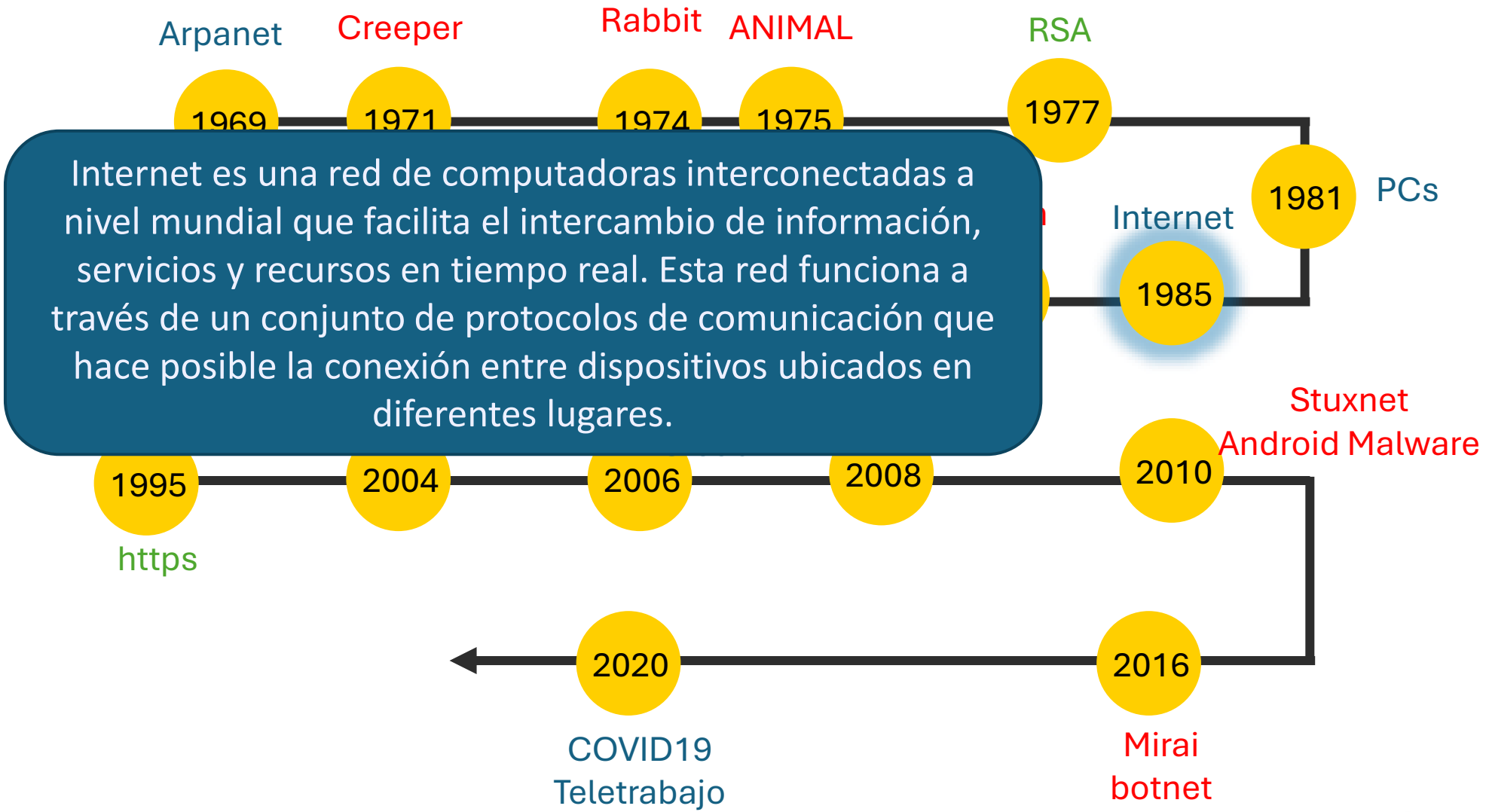
La clave pública se puede distribuir libremente y se usa para cifrar los mensajes. La clave privada, que debe mantenerse en secreto, se usa para descifrar los mensajes cifrados con la clave pública correspondiente.



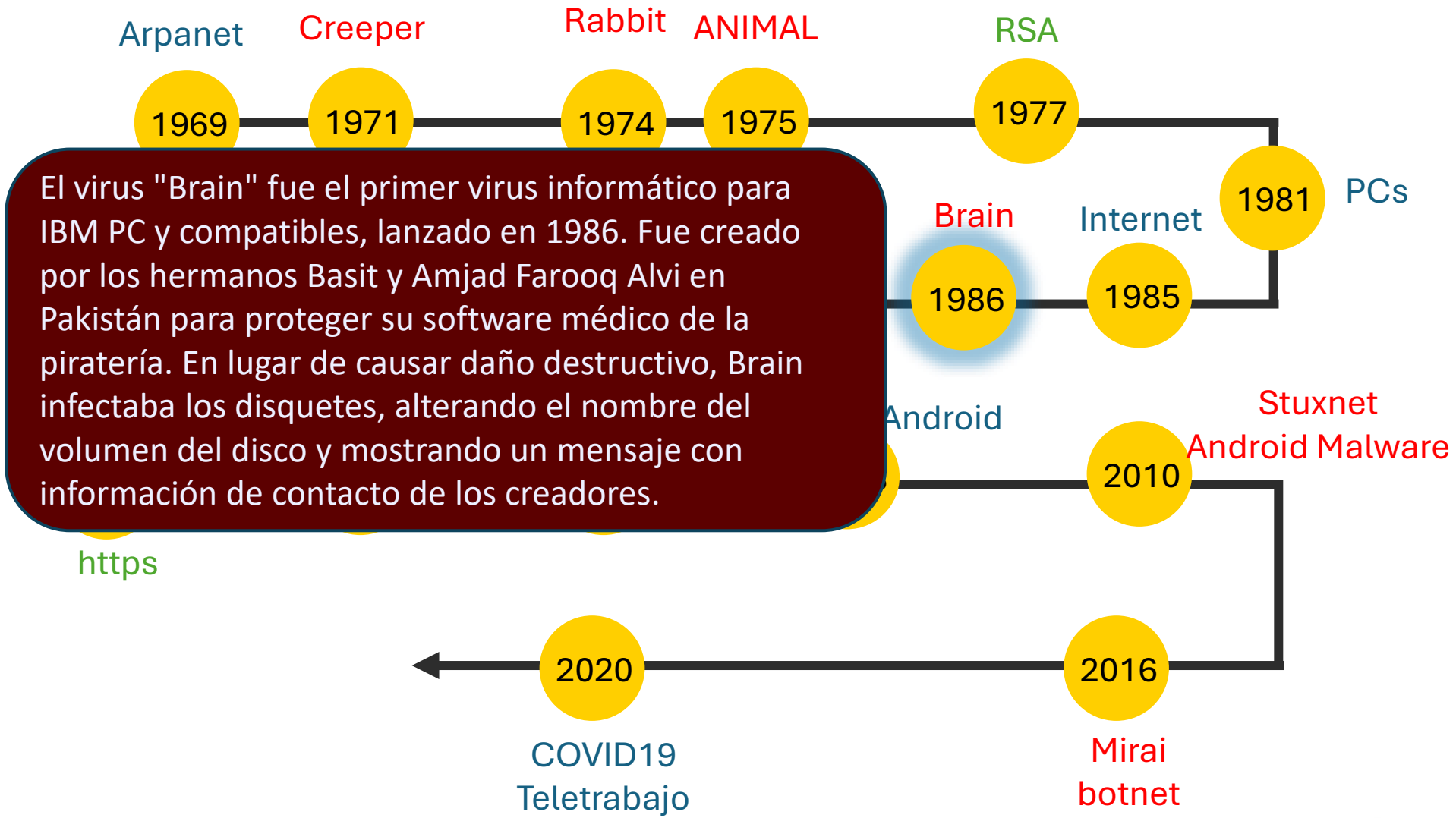
Factores sobresalientes en la evolución de la Ciberseguridad



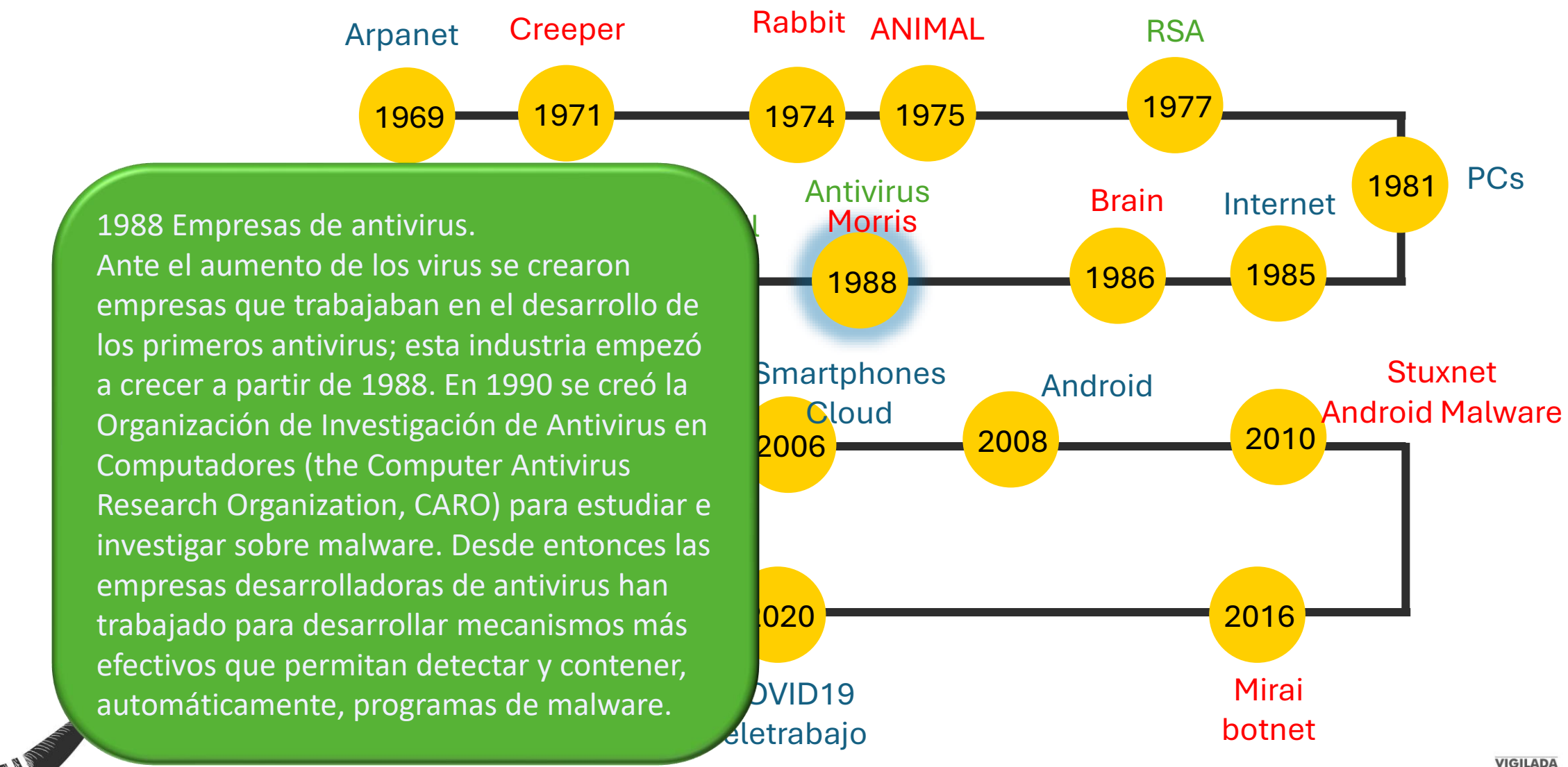
Factores sobresalientes en la evolución de la Ciberseguridad



Factores sobresalientes en la evolución de la Ciberseguridad

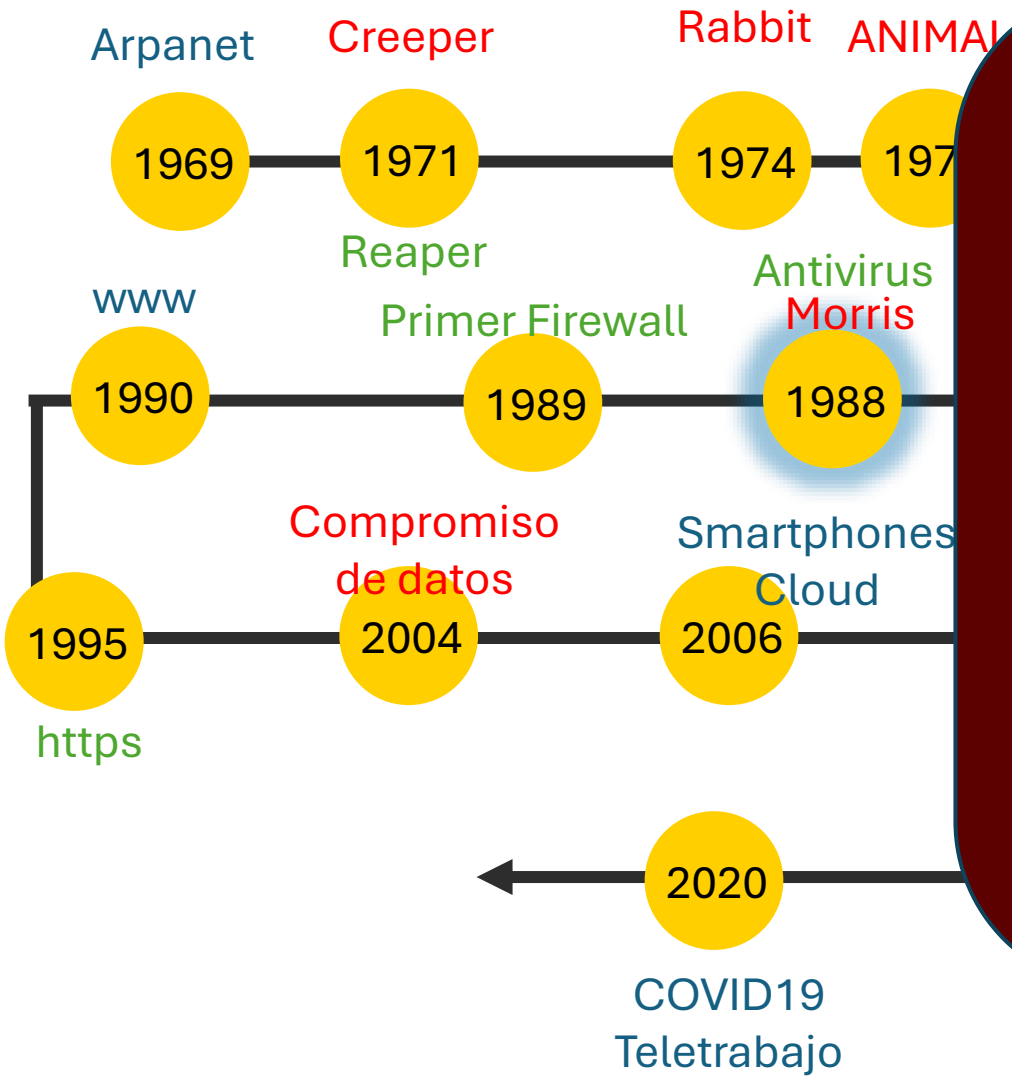


Factores sobresalientes en la evolución de la Ciberseguridad



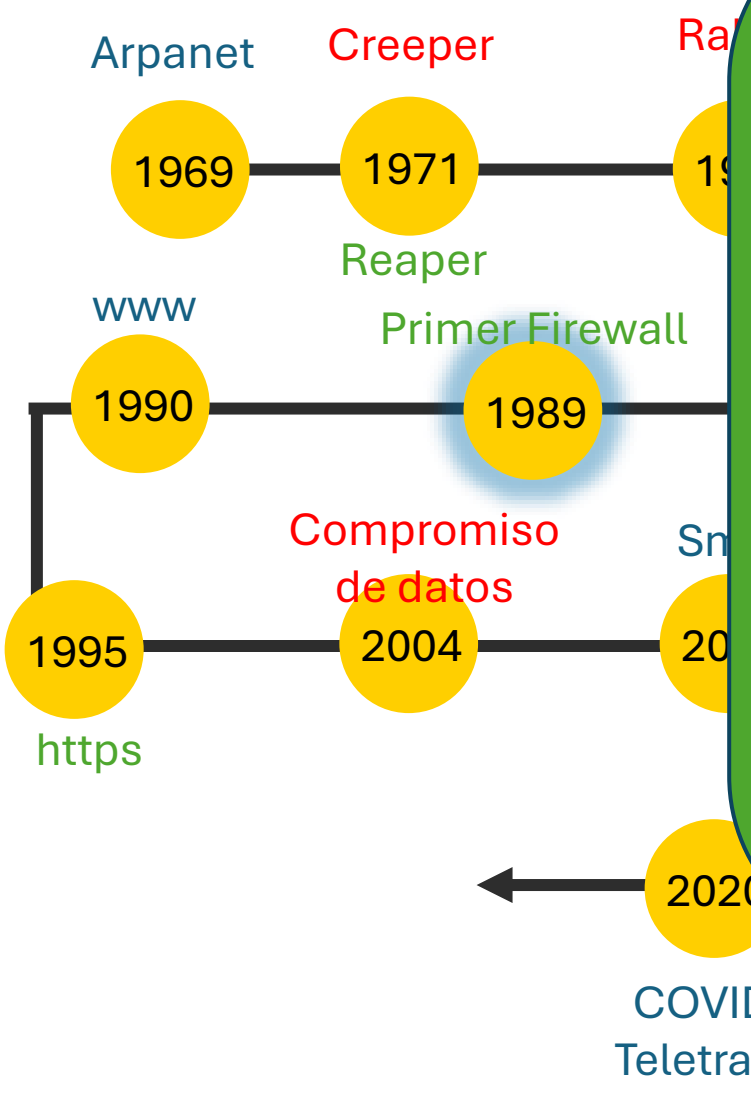
1988 Empresas de antivirus.
Ante el aumento de los virus se crearon empresas que trabajaban en el desarrollo de los primeros antivirus; esta industria empezó a crecer a partir de 1988. En 1990 se creó la Organización de Investigación de Antivirus en Computadores (the Computer Antivirus Research Organization, CARO) para estudiar e investigar sobre malware. Desde entonces las empresas desarrolladoras de antivirus han trabajado para desarrollar mecanismos más efectivos que permitan detectar y contener, automáticamente, programas de malware.

Factores sobresalientes en la evolución de la Ciberseguridad



1988 Morris.
Un estudiante de doctorado desarrolla un programa, considerado el primer gusano, que explota vulnerabilidades en los sistemas Unix para ingresar de forma automatizada y no autorizada a un sistema. El programa se replica y se propagaba de forma autónoma (no requiere intervención del usuario) sobrecargando los sistemas que atacaba. El gusano se propagó por medio de internet, alcanzando en un par de horas cientos de computadores conectados y dejándolos sin capacidad de respuesta. Este caso muestra la gran velocidad de propagación del malware cuando no requiere intervención humana y las consecuencias potenciales de dicha propagación. (Tanenbaum, Sistemas Operativos Modernos, 2009).

Factores sobresalientes en la evolución de la Ciberseguridad

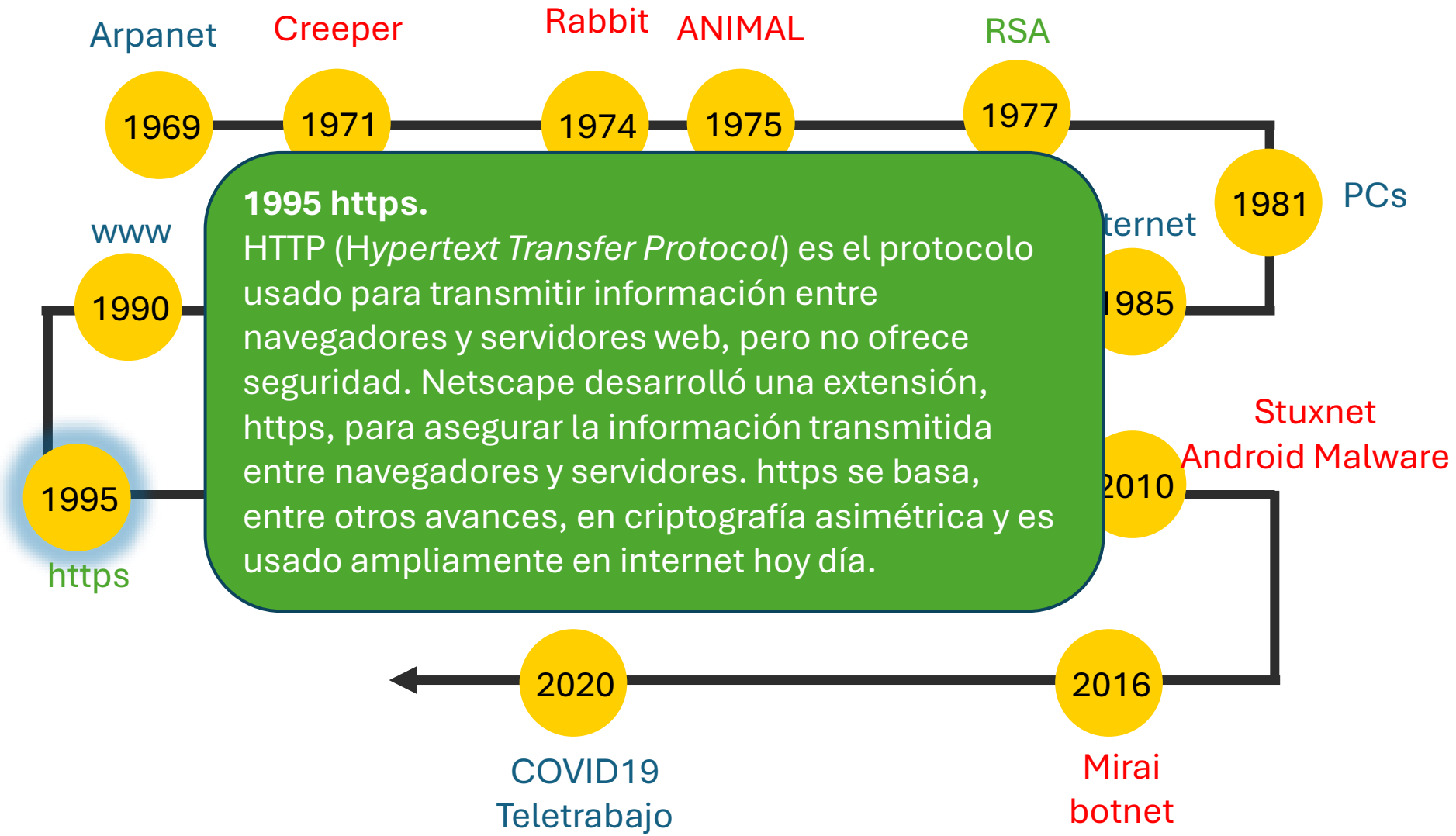


1989 – 1990. Primer firewall y primer IDS.

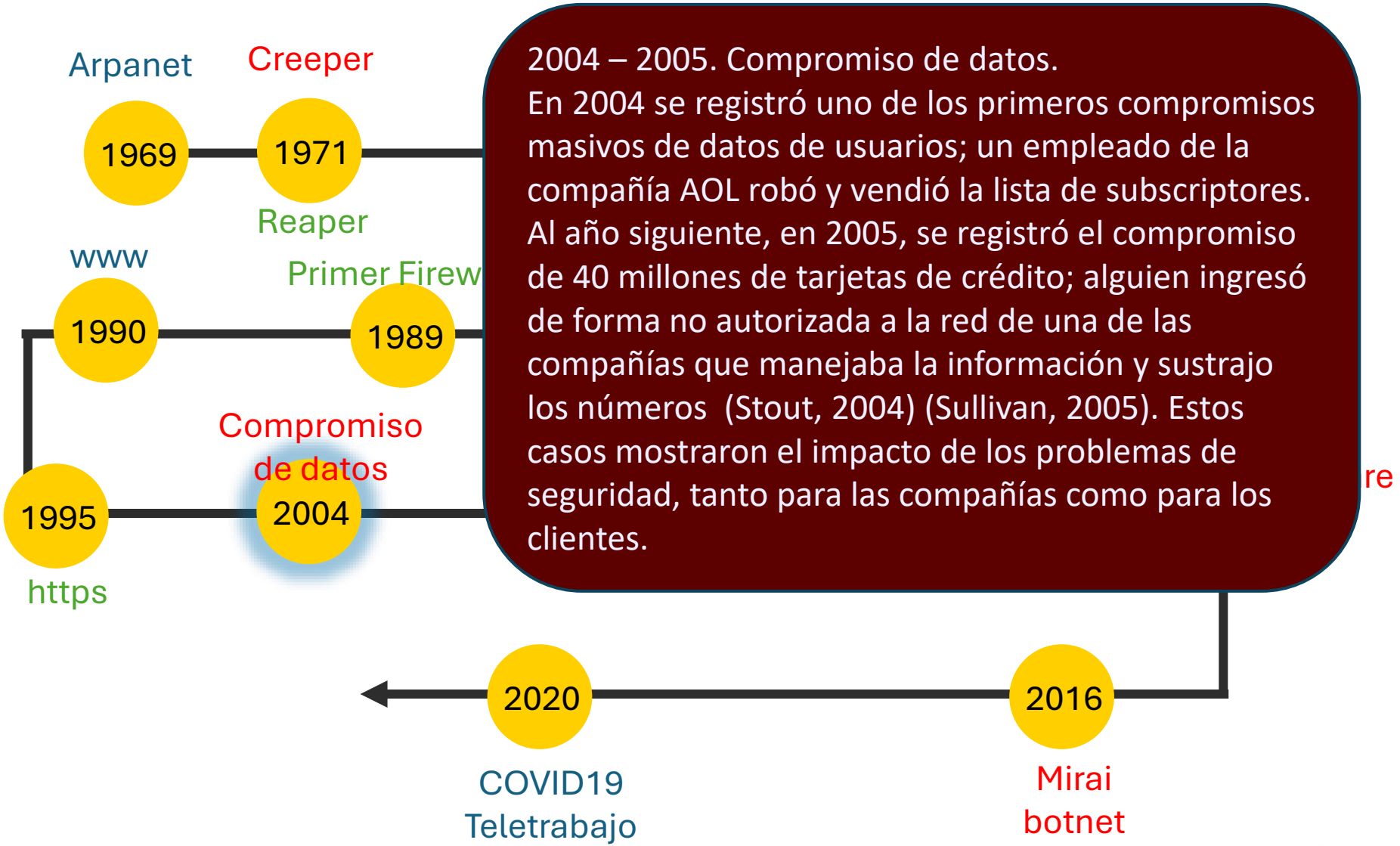
En 1989 aparece el primer trabajo de investigación que presenta un programa que filtra los paquetes de red. En un punto de ingreso revisa el contenido de los paquetes y dependiendo de la fuente y destino decide si los deja pasar o no. En los años siguientes fueron apareciendo firewalls que consideraban información adicional para tomar decisiones; no solo la fuente y el destino de un paquete. En 1990 aparece el primer trabajo de investigación que presenta un sistema experto entrenado para detectar actividad maliciosa conocida. Estos desarrollos se unen a los avances logrados por las empresas de antivirus. (Mogul, 1989) (Lunt, y otros, 1990).

Factores sobresalientes en la evolución de la Ciberseguridad

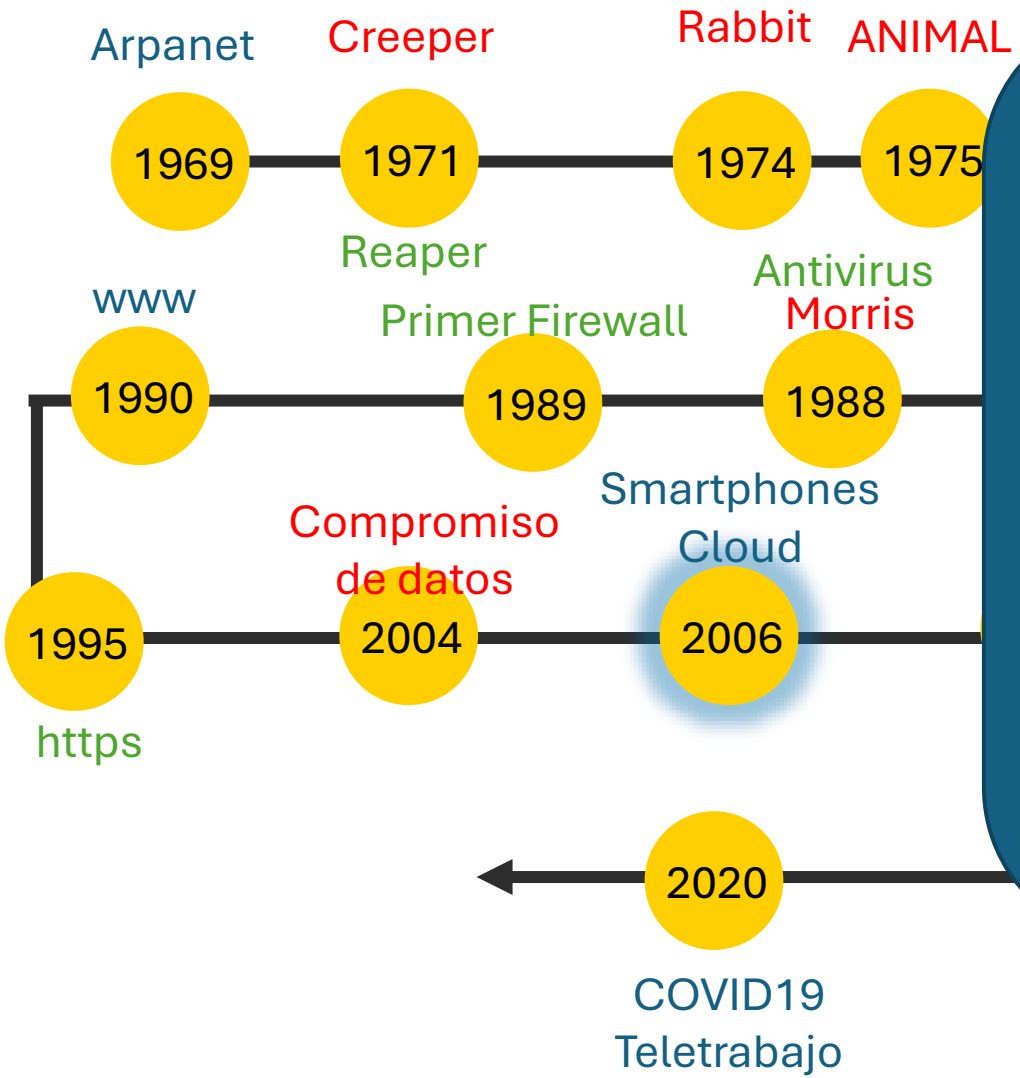
Factores sobresalientes en la evolución de la Ciberseguridad



Factores sobresalientes en la evolución de la Ciberseguridad

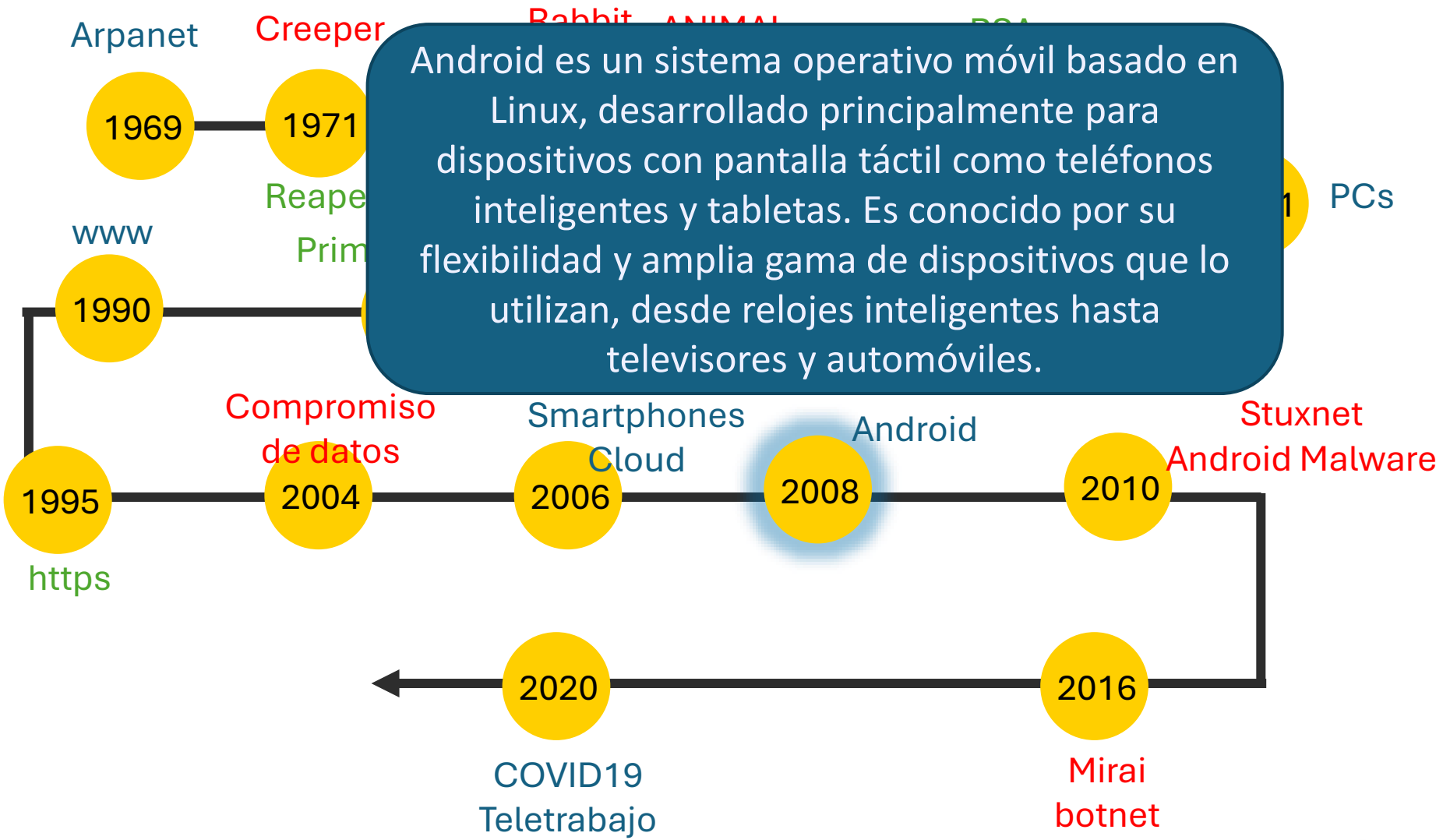


Factores sobresalientes en la evolución de la Ciberseguridad

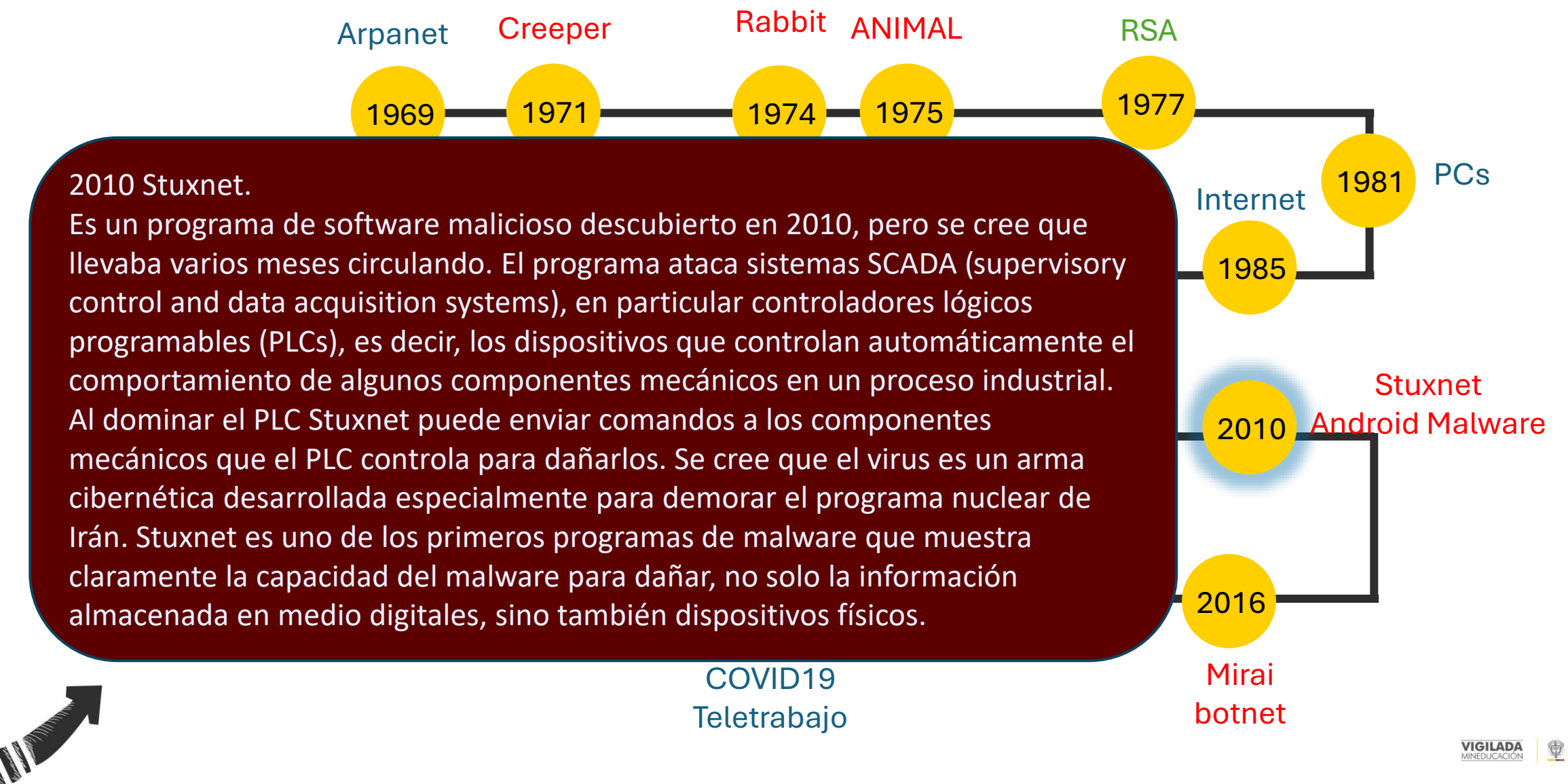


La computación en la nube (cloud computing) es fundamental para los smartphones modernos, permitiendo el almacenamiento de datos, ejecución de aplicaciones y sincronización entre dispositivos. Los usuarios pueden acceder a servicios como Google Drive, iCloud o Samsung Cloud para almacenar fotos, videos y documentos, liberando espacio en sus dispositivos móviles. Además, la nube facilita la ejecución de aplicaciones complejas y la sincronización de datos en tiempo real, mejorando la experiencia del usuario móvil.

Factores sobresalientes en la evolución de la Ciberseguridad

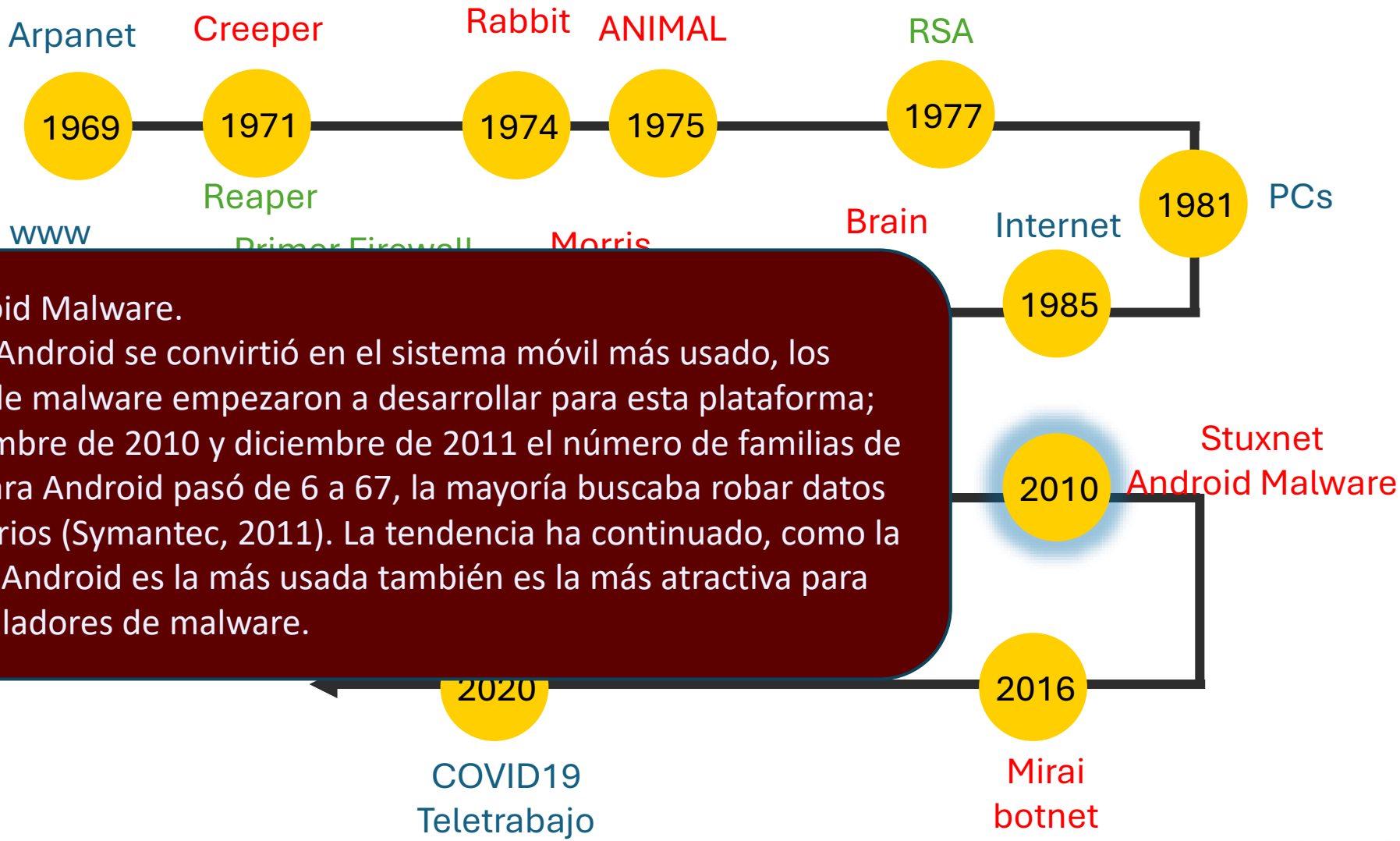


Factores sobresalientes en la evolución de la Ciberseguridad



2010 Stuxnet.
Es un programa de software malicioso descubierto en 2010, pero se cree que llevaba varios meses circulando. El programa ataca sistemas SCADA (supervisory control and data acquisition systems), en particular controladores lógicos programables (PLCs), es decir, los dispositivos que controlan automáticamente el comportamiento de algunos componentes mecánicos en un proceso industrial. Al dominar el PLC Stuxnet puede enviar comandos a los componentes mecánicos que el PLC controla para dañarlos. Se cree que el virus es un arma cibernética desarrollada especialmente para demorar el programa nuclear de Irán. Stuxnet es uno de los primeros programas de malware que muestra claramente la capacidad del malware para dañar, no solo la información almacenada en medio digitales, sino también dispositivos físicos.

Factores sobresalientes en la evolución de la Ciberseguridad



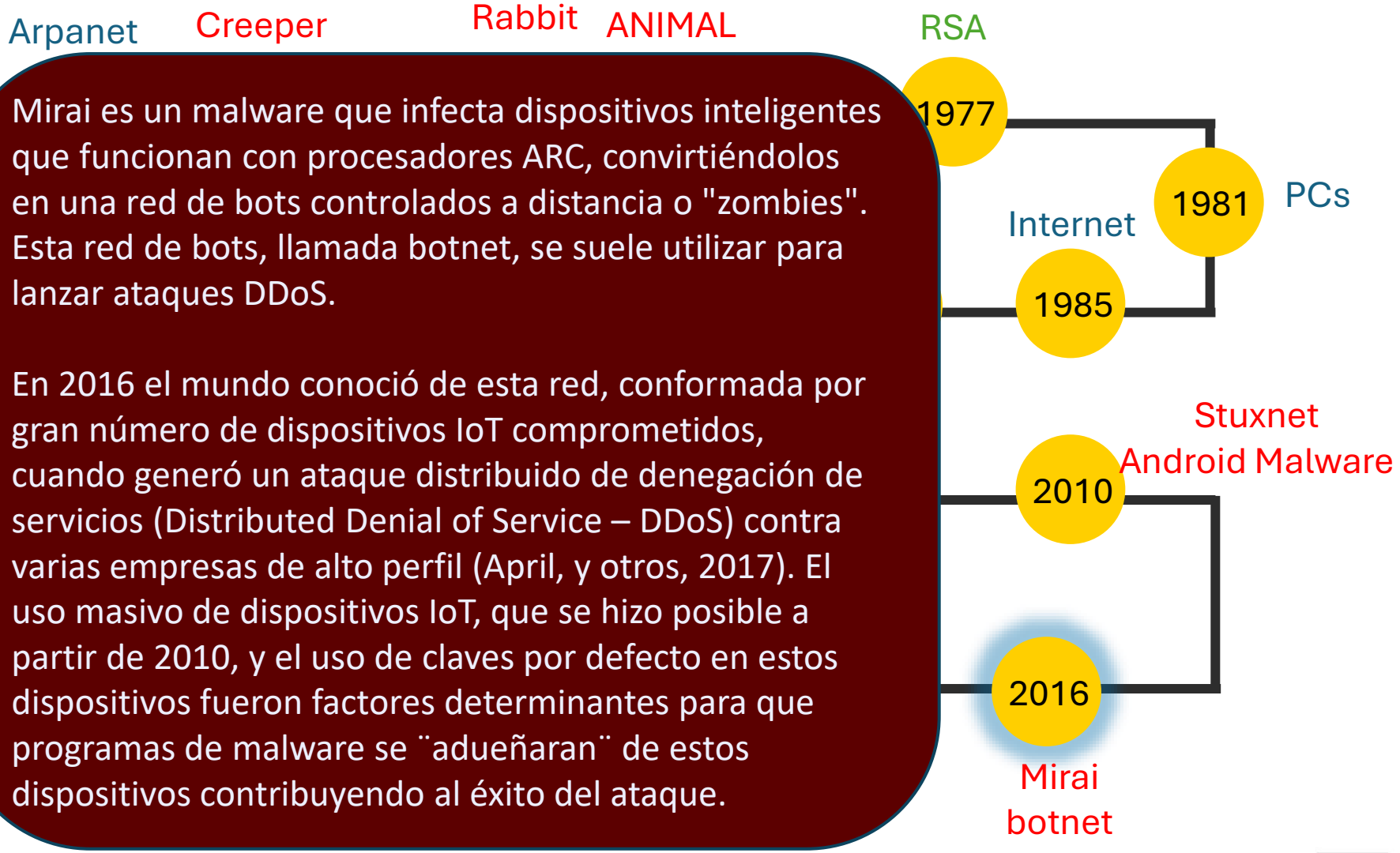
2010 Android Malware.

Cuando Android se convirtió en el sistema móvil más usado, los creadores de malware empezaron a desarrollar para esta plataforma; entre diciembre de 2010 y diciembre de 2011 el número de familias de malware para Android pasó de 6 a 67, la mayoría buscaba robar datos de los usuarios (Symantec, 2011). La tendencia ha continuado, como la plataforma Android es la más usada también es la más atractiva para los desarrolladores de malware.

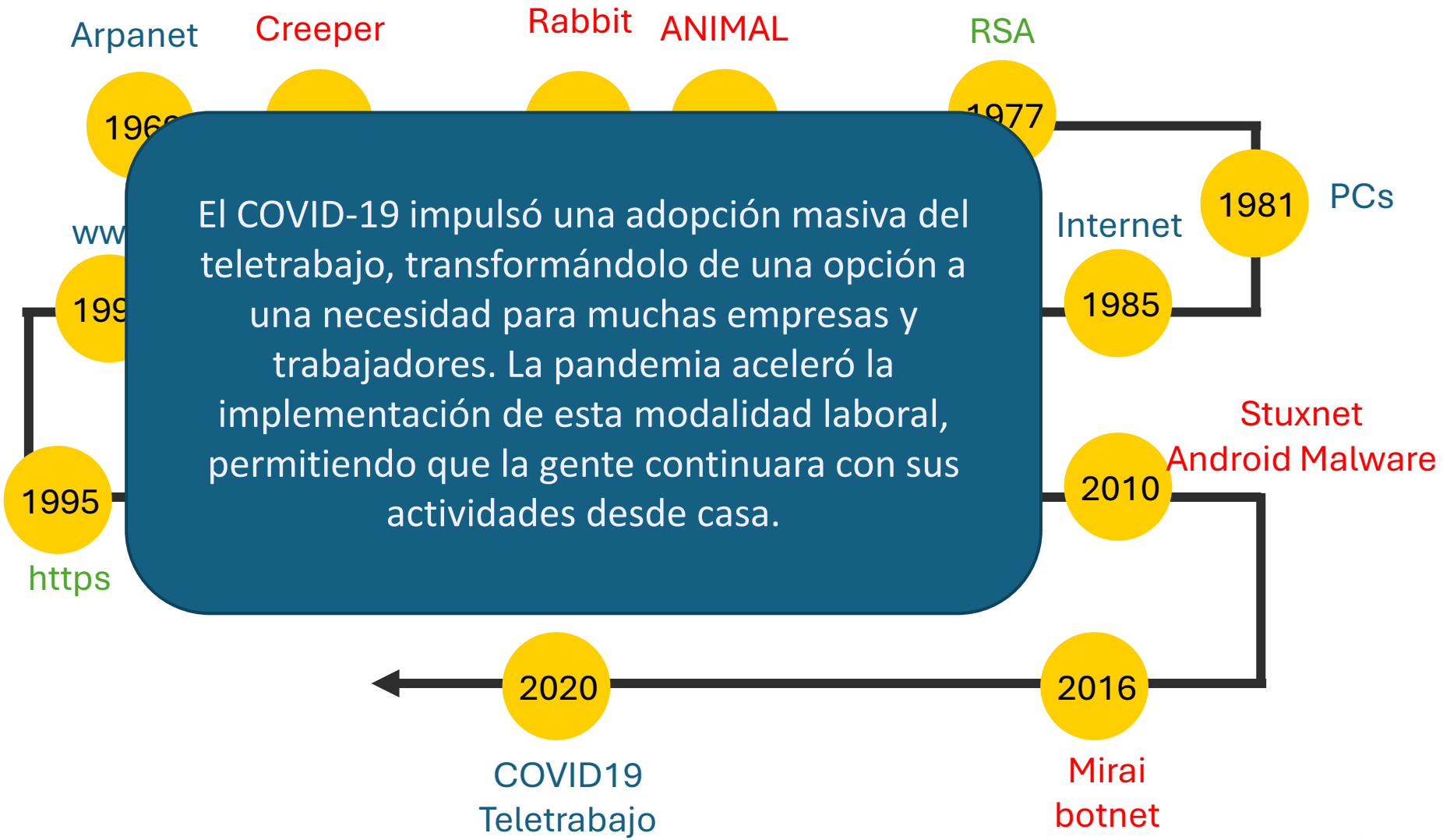
Factores sobresalientes en la evolución de la Ciberseguridad

Mirai es un malware que infecta dispositivos inteligentes que funcionan con procesadores ARC, convirtiéndolos en una red de bots controlados a distancia o "zombies". Esta red de bots, llamada botnet, se suele utilizar para lanzar ataques DDoS.

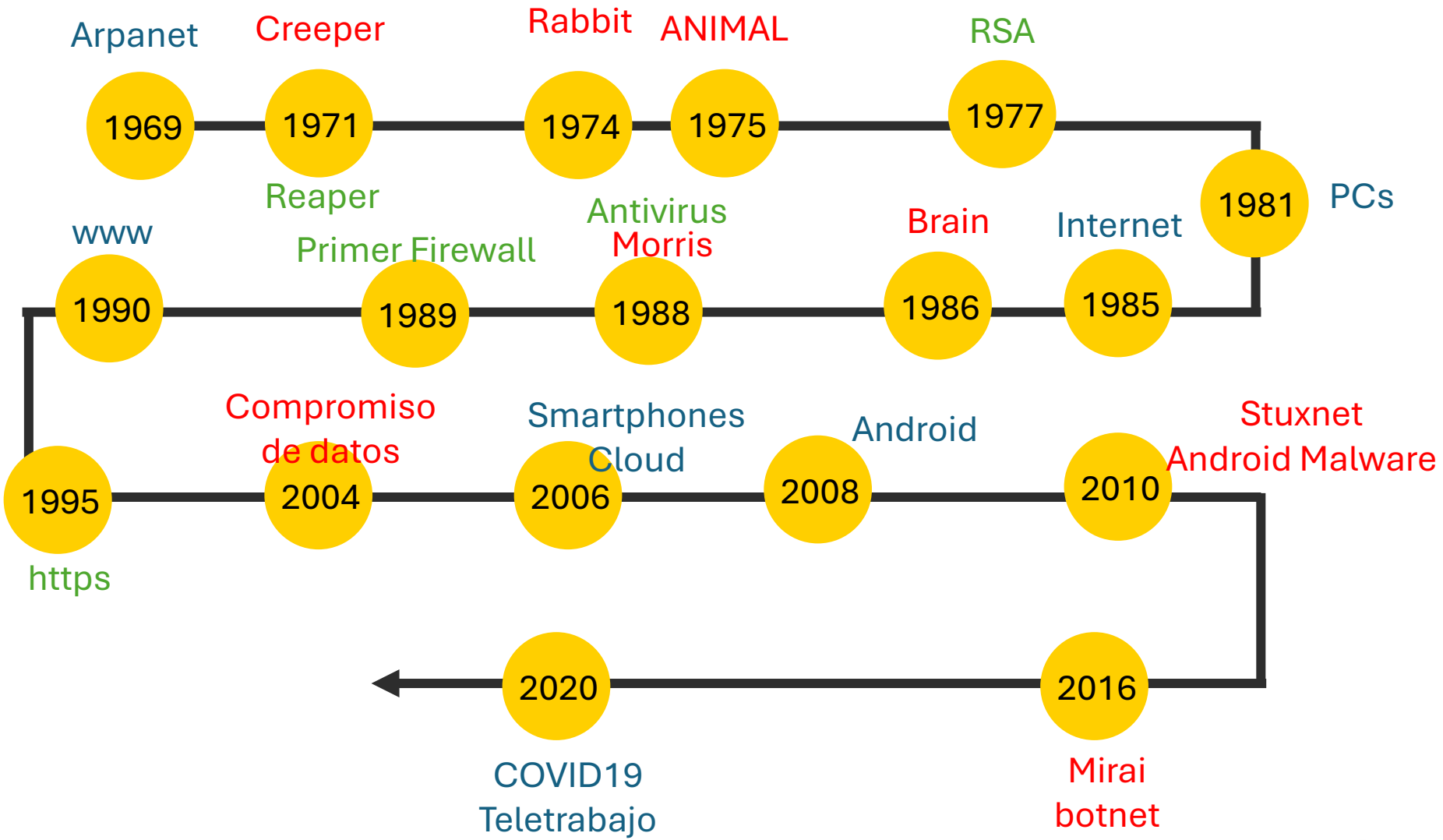
En 2016 el mundo conoció de esta red, conformada por gran número de dispositivos IoT comprometidos, cuando generó un ataque distribuido de denegación de servicios (Distributed Denial of Service – DDoS) contra varias empresas de alto perfil (April, y otros, 2017). El uso masivo de dispositivos IoT, que se hizo posible a partir de 2010, y el uso de claves por defecto en estos dispositivos fueron factores determinantes para que programas de malware se ¨adueñaran¨ de estos dispositivos contribuyendo al éxito del ataque.



Factores sobresalientes en la evolución de la Ciberseguridad



Factores sobresalientes en la evolución de la Ciberseguridad



¿Por qué es importante?

Pérdida de datos

Ransomware

Colonial Pipeline (2021)

Eliminación de backups

Code Spaces (2014)

Borrado malicioso

GitHub (2018)

¿Por qué es importante?

Robo de identidad

Filtración de credenciales

LinkedIn (2012 y 2021)

Phishing masivo

Google Docs phishing (2017)

Ataques a gobiernos

Estonia (2007)

¿Por qué es importante?

Fraudes bancarios

Skimming digital

Malware Carbanak (2013-2016)

Ataques a FinTechs

Ing. social Robinhood (2020)

Clonación de tarjetas

El caso Target (2013)

¿Por qué es importante?

Interrupción de servicios

Ataques DDoS

Dyn (2016)

Sabotaje industrial

El malware Triton (2017)

Ataques a infraestructura

Ciberataques a hospitales

¿Por qué es importante?

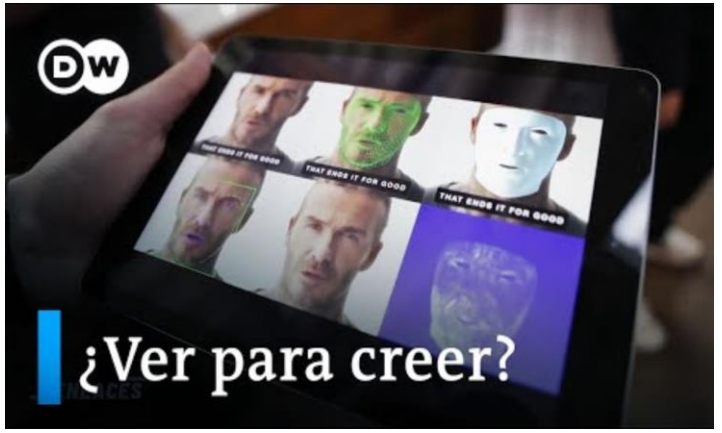
Otros impactos graves

Espionaje corporativo

SolarWinds (2020)

Sabotaje industrial

El malware Triton (2017)



Diferencia entre Seguridad de la Información y Ciberseguridad

Confidencialidad

Garantiza que solo personas autorizadas accedan a la información.
Ejemplo: Contraseñas protegidas.

Integridad

Asegura que la información no sea alterada.
Ejemplo: Firma digital.

Disponibilidad

Asegura que la información esté accesible cuando se necesita.
Ejemplo: Servidor activo 24/7

Confidencialidad

Correo electrónico corporativo

Escenario:
Una empresa envía correos electrónicos con información estratégica (por ejemplo, planes de expansión) a través de una red Wi-Fi pública sin cifrado.

Problema:
Un atacante intercepta los correos usando un sniffer en la red Wi-Fi, accediendo a información confidencial.

Consecuencia:
El atacante podría vender los planes a un competidor, causando una fuga de información.

Solución:
cifrar los correos y una VPN para proteger la conexión en redes públicas.

Integridad

Alteración de una página web gubernamental

Escenario:
Un atacante explota una vulnerabilidad en un servidor web de una entidad gubernamental y modifica el contenido de una página que publica información sobre beneficios sociales.

Problema:
Los ciudadanos ven información falsa (por ejemplo, requisitos incorrectos para un subsidio), lo que lleva a decisiones erróneas.

Consecuencia:
Pérdida de confianza en la entidad y confusión pública.

Solución:
Implementar controles de integridad como firmas digitales o hashes para detectar cambios no autorizados y auditorías regulares del servidor.

Disponibilidad

Falla en un sistema hospitalario

Escenario:
Un hospital depende de un sistema electrónico para acceder a los historiales médicos. Un ransomware cifra los servidores, dejando los datos inaccesibles.

Problema:
Los médicos no pueden acceder a información crítica, afectando la disponibilidad y retrasando tratamientos.

Consecuencia:
Riesgo para la salud de los pacientes y posibles demandas legales.

Solución:
Mantener copias de seguridad actualizadas en un entorno offline y usar sistemas de detección de intrusos para prevenir ransomware.

Ejercicio 1: Clasifica acciones según el modelo CIA

Lee las siguientes acciones y clasifícalas según comprometen la **Confidencialidad** (C), **Integridad** (I) o **Disponibilidad** (D):

a. Un hacker accede a una base de datos sin permiso

b. Un virus altera los datos de un informe

c. Un ataque deja fuera de línea el correo corporativo

Ejercicio 2: Mini caso

Enunciado: Una empresa envía un correo electrónico masivo a todos sus clientes. Por error, no utiliza la opción “Copia oculta” (CCO) y expone visiblemente todas las direcciones de correo de los destinatarios. Uno de los clientes nota esto y se queja, argumentando que se ha puesto en riesgo su privacidad.

Pregunta

¿Qué principio del modelo CIA se vulnera y por qué?

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. National Institute of Standards, NIST. (s.f.). *Glosario*. Recuperado el Mayo de 2021, de https://csrc.nist.gov/glossary
6. Pasado, presente y futuro de la seguridad de la información. (s/f). Incibe.es. Recuperado el 12 de agosto de 2025, de https://www.incibe.es/empresas/blog/pasado-presente-y-futuro-de-la-seguridad-de-la-informacion
7. Harford, T. (s.f.). *La tecnología de espionaje de la guerra fría que todos usamos*. Recuperado el Mayo de 2021, de BBC News: https://www.bbc.com/mundo/noticias-49442319
8. Sullivan, B. (Junio de 2005). *40 million credit cards exposed*. Obtenido de NBC News: https://www.nbcnews.com/id/wbna8260050