50 años conviviendo con los virus informáticos: *Una breve historia del malware*

Ricardo J. Rodríguez

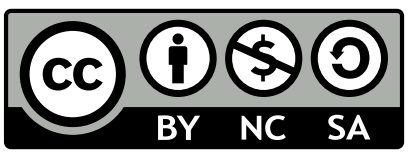
rjrodriguez@unizar.es ※ @RicardoJRdez ※ www.ricardojrodriguez.es

Universidad Zaragoza

Dpto. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza, España

23 de julio, 2021

RetroEuskal
(online)



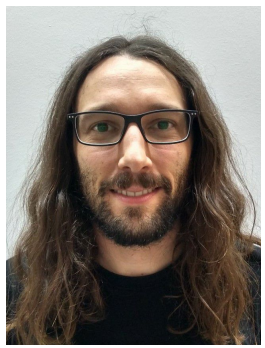
$whoami

- **Profesor Contratado Doctor, Universidad de Zaragoza**
- **Líneas de investigación**:
  - Análisis de sistemas (seguridad, rendimiento, resiliencia)
  - Análisis de software
  - Análisis forense digital
- Speaker y profesor de talleres en conferencias del sector (NcN, HackLU, RootedCON, STIC CCN-CERT, HIP, MalCON, HITB. . .)

Universidad Zaragoza

$whoami

- **Profesor Contratado Doctor, Universidad de Zaragoza**
- **Líneas de investigación**:
  - Análisis de sistemas (seguridad, rendimiento, resiliencia)
  - Análisis de software
  - Análisis forense digital
- Speaker y profesor de talleres en conferencias del sector (NcN, HackLU, RootedCON, STIC CCN-CERT, HIP, MalCON, HITB. . .)
- **Equipo de investigación** – *¡hacemos cosas chulas!*
  - `https://reversea.me` / `https://t.me/reverseame`



Miguel Martín-Pérez

Daniel Uroz

Razvan Raducu

Universidad Zaragoza

Índice

Universidad Zaragoza

Índice

Universidad Zaragoza

Introducción

Malware

Mal*icious soft***ware**

- **Código dañino** (RD 43/2021, BOE-A-2021-1192)
- "*Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como malware. Así pues malware es un término que engloba varios tipos de programas dañinos.*"

Universidad Zaragoza

Introducción

Malware

Mal*icious soft***ware**

- **Código dañino** (RD 43/2021, BOE-A-2021-1192)
- "*Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como malware. Así pues malware es un término que engloba varios tipos de programas dañinos.*"
- `s/virus/malware/` en el título 🙂

Introducción
Virus

- **Necesita un anfitrión** (al que infecta): ficheros del sistema
- **Capacidad de autorreplicación**

Universidad Zaragoza

Introducción
Virus

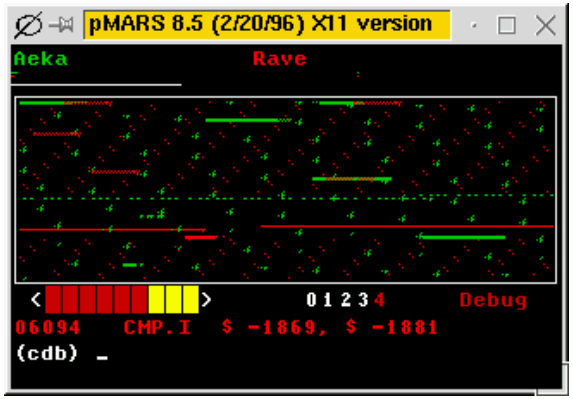
- **Necesita un anfitrión** (al que infecta): ficheros del sistema
- **Capacidad de autorreplicación**

John von Neumann

- Diversas charlas entre 1948-1949, presentando partes de la **teoría de automátas auto-reproducibles**
- "*Theory of Self-Reproducing Automata*"(`http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf`), 1966

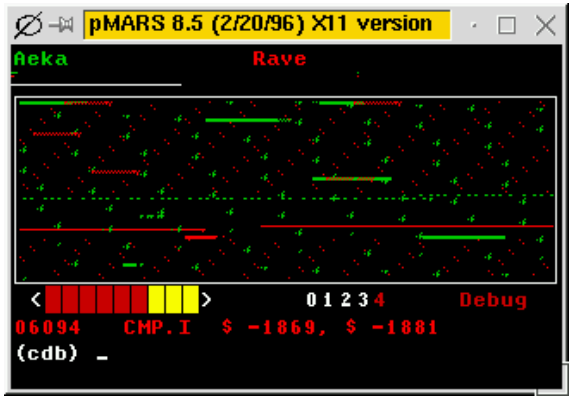
Universidad Zaragoza

Introducción
Virus

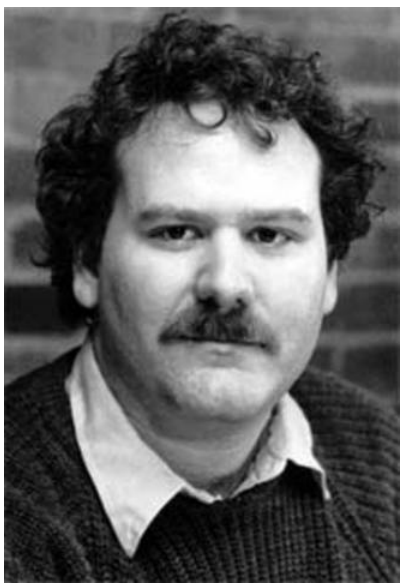


- En 1959, crean `CoreWar` en Bell Computer Labs
- **Juego basado en la teoría de von Neumann**
  - Los programas combaten entre sí para ocupar toda la memoria, eliminando así a los oponentes

Introducción
Virus



- En 1959, crean `CoreWar` en Bell Computer Labs
- **Juego basado en la teoría de von Neumann**
  - Los programas combaten entre sí para ocupar toda la memoria, eliminando así a los oponentes



Fred Cohen

- Tesis en 1984: **define el término virus**
- "*A program that can infect other programs by modifying them to include a, possibly evolved, version of itself*"

Índice

Universidad Zaragoza

Evolución

Primera etapa: 70s

1970 — 1971 — 1972 — 1973 — 1974 — 1975 — 1976 — 1977 — 1978 — 1979

Creeper

Wabbit

ANIMAL

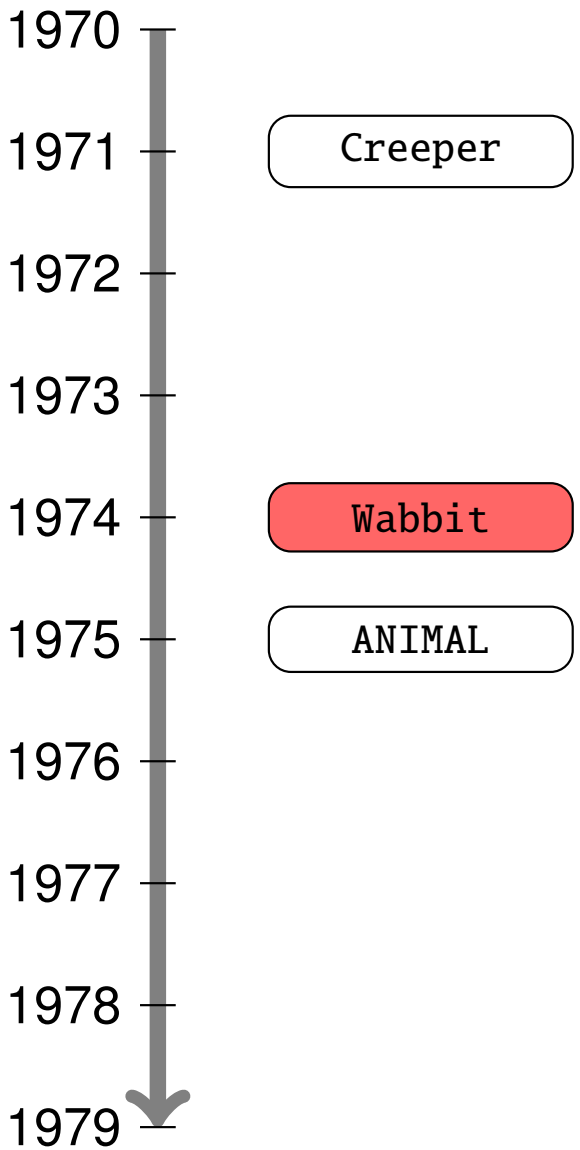
- Creeper
  - **Prueba de concepto** desarrollada por Bob Thomas (BBN Technologies)
  - TENEX OS sobre sistemas DEC PDP-10
  - Más bien **gusano**: propagación por la red
  - Programa para eliminarlo: *The Reaper*

```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER      SUBSYS
1   DET  SYSTEM    NETSER
2   DET  SYSTEM    TIPSER
3   12   RT        EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

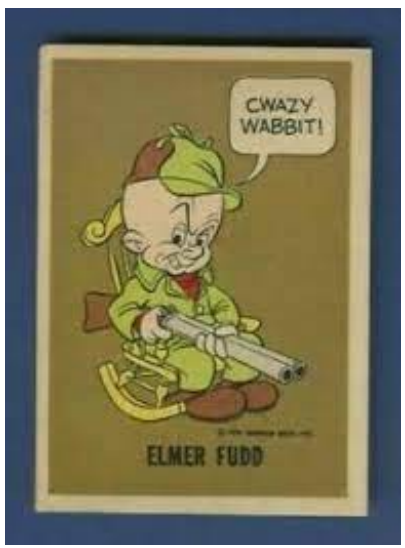
Universidad Zaragoza

Evolución

Primera etapa: 70s

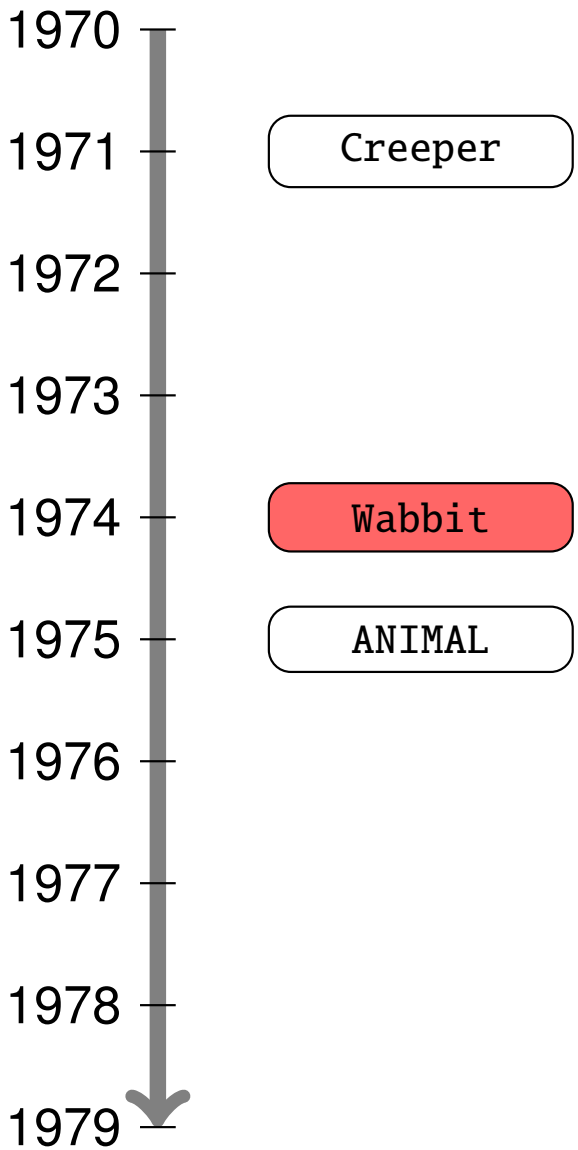


- `Creeper`
- `Wabbit`
  - Sistemas IBM OS/360 mainframe
  - Se autorreplicaba hasta colgar el sistema (**denegación de servicio**, DoS)
  - **Bomba *fork***



Evolución

Primera etapa: 70s

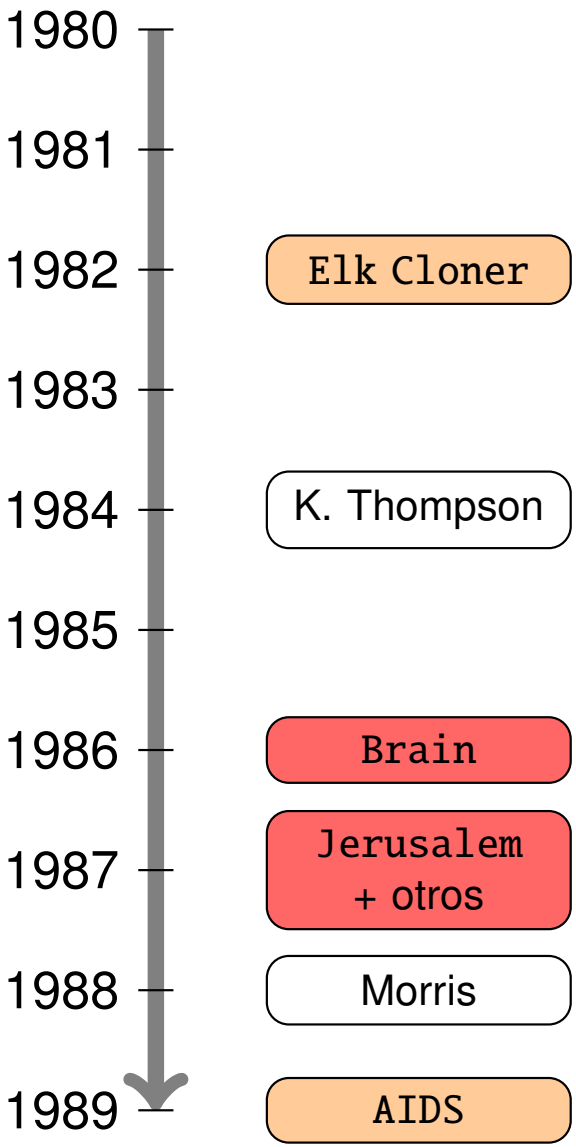


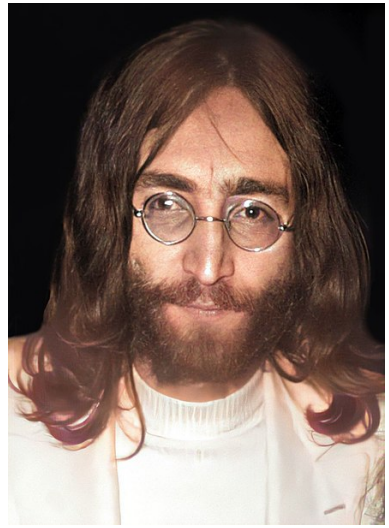
- Creeper
- Wabbit
- ANIMAL+PERVADE (John Walker)
  - Sistemas UNIVAC 1108
  - ANIMAL: programa interactivo con el usuario (pregunta y respuesta). PERVADE hacía una copia de ambos en todos los directorios del usuario
  - **No dañino**. Considerado como el **primer troyano**
  - http://www.fourmilab.ch/documents/univac/animal.html

```
.
.       THE TAG 'TALK' MAY BE SET NONZERO TO GENERATE DIAGNOSTIC
.       OUTPUT DURING THE OPERATION OF PERVADE.
.
TALK    EQU     0                   TURN IT OFF
.
.       TIME IN SECONDS USED TO IDENTIFY PERVADE-INSERTED ELEMENTS.
.
TIMEFLAG EQU    25*60*60+14*60+19   25:14:19
.
.
        AXR$
        DEFUNCT$
        LIT$    2
.
.       PROC USED TO CHECK FOR FORCIBLE TERMINATION
.
P       PROC    0,2                 CHECK FOR TERMINATION OF MAIN PROGRAM
YET*    NAME    0
        TZ      PVSTOP              IS THE CEASE FLAG SET ?
        J       PERVEX              YES.  GET OUT OF HERE
        END
.
.       PROC TO LOAD REASON FOR IGNORING FILE IN TALK MODE
.
P       PROC    *1
REASON* NAME    0
        ON      TALK
        LR      R2,(LJSF$1 P(1,1))  LOAD REASON FOR SKIPPING FILE
        OFF     TALK
        END     .
```

Evolución

Segunda etapa: 80s



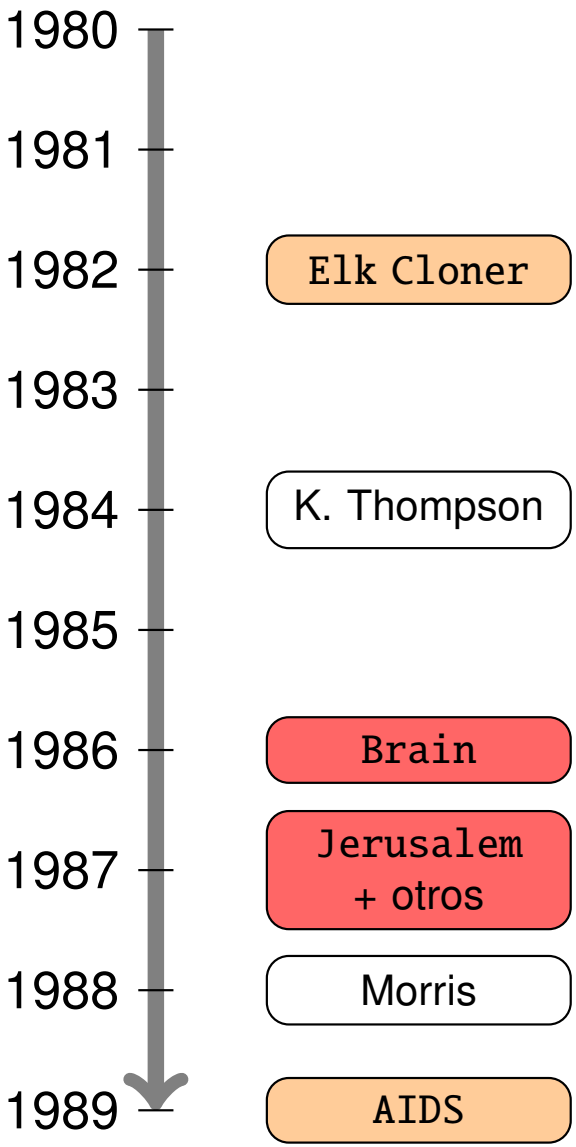


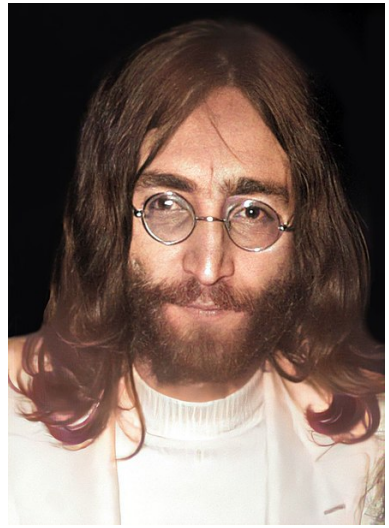
- `Elk Cloner` (Richard Skrenta)
  - Sistemas Apple II
  - **Infección de disquetes**, con 15 comportamientos "maliciosos"
  - Lectura: `https://arxiv.org/abs/2007.15759`

```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

Evolución

Segunda etapa: 80s

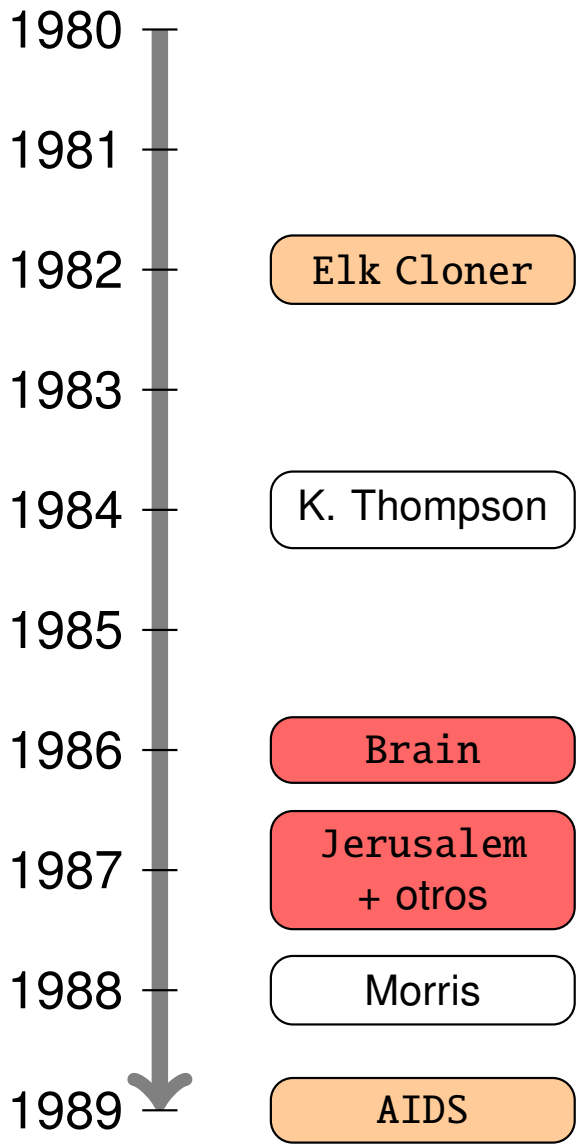


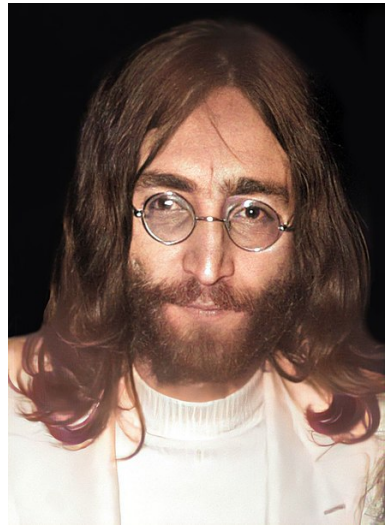


- `Elk Cloner` (Richard Skrenta)
- Ken Thompson
  - Compilador de C *especial* para `login`
  - **Primer backdoor**
  - doi: 10.1145/358198.358210 (*Turing Award lecture*)

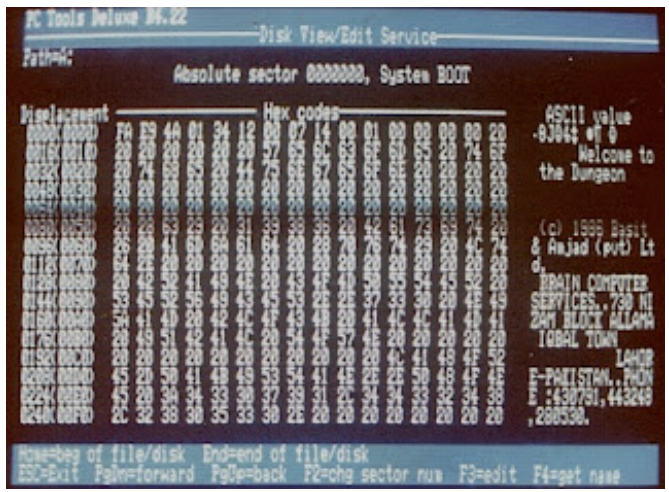
Evolución

Segunda etapa: 80s



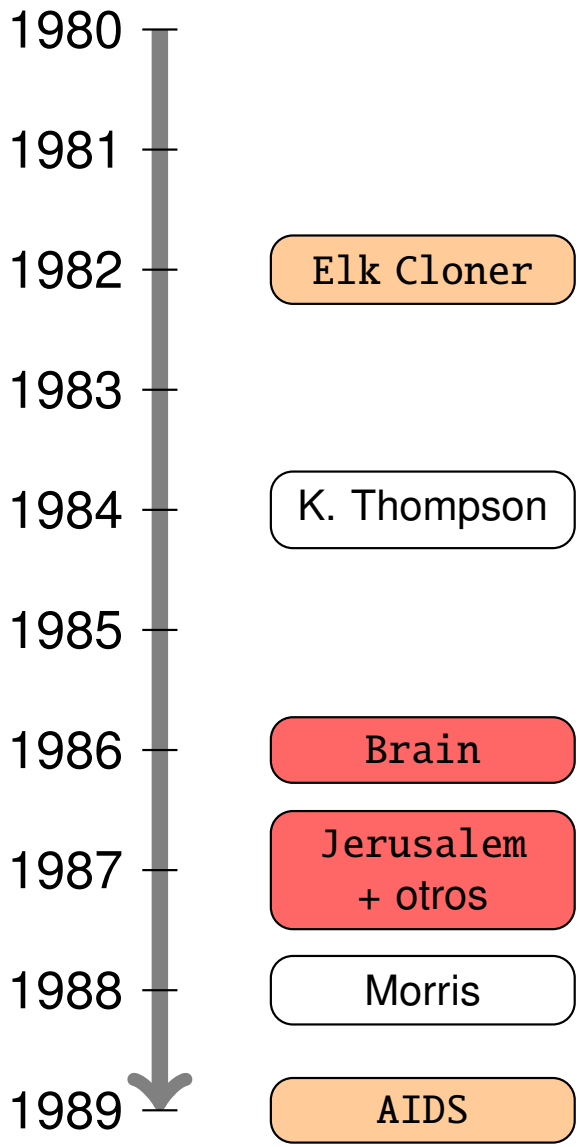


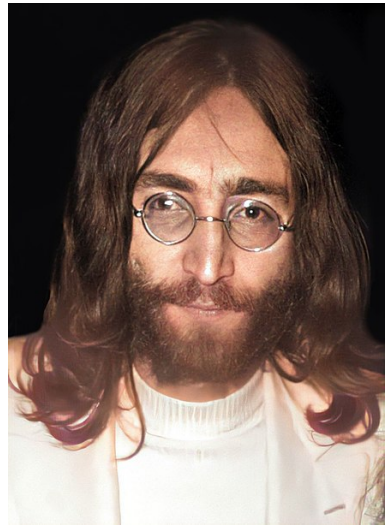
- `Elk Cloner` (Richard Skrenta)
- Ken Thompson
- `Brain` (Basit y Amjad Farooq Ali)
  - **Primer virus para IBM/PC**
  - Reemplazaba el sector de arranque de disquetes
  - Inspiración de John McAfee: crea VirusScan



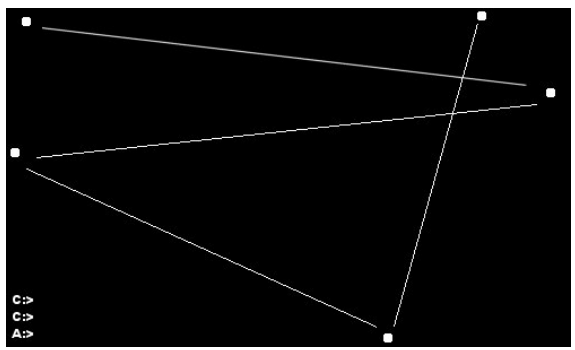
Evolución

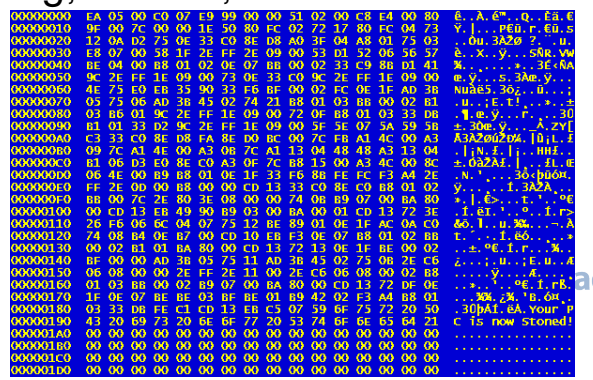
Segunda etapa: 80s





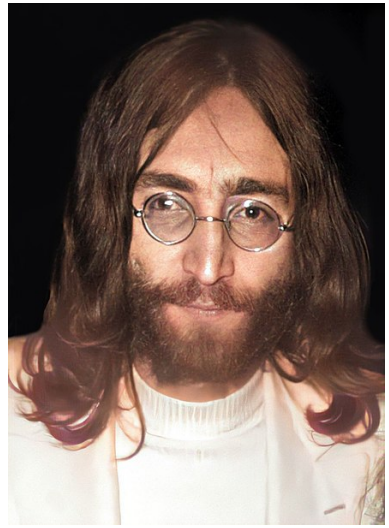
- `Elk Cloner` (Richard Skrenta)
- Ken Thompson
- `Brain` (Basit y Amjad Farooq Ali)
- `Jerusalem` y más virus de sector de arranque
  - Sistema DOS
  - Activado el viernes 13
  - **Destruía ficheros COM (y algunos EXE)**
  - **Más boot sectors**: Ping-pong, Stoned, ...

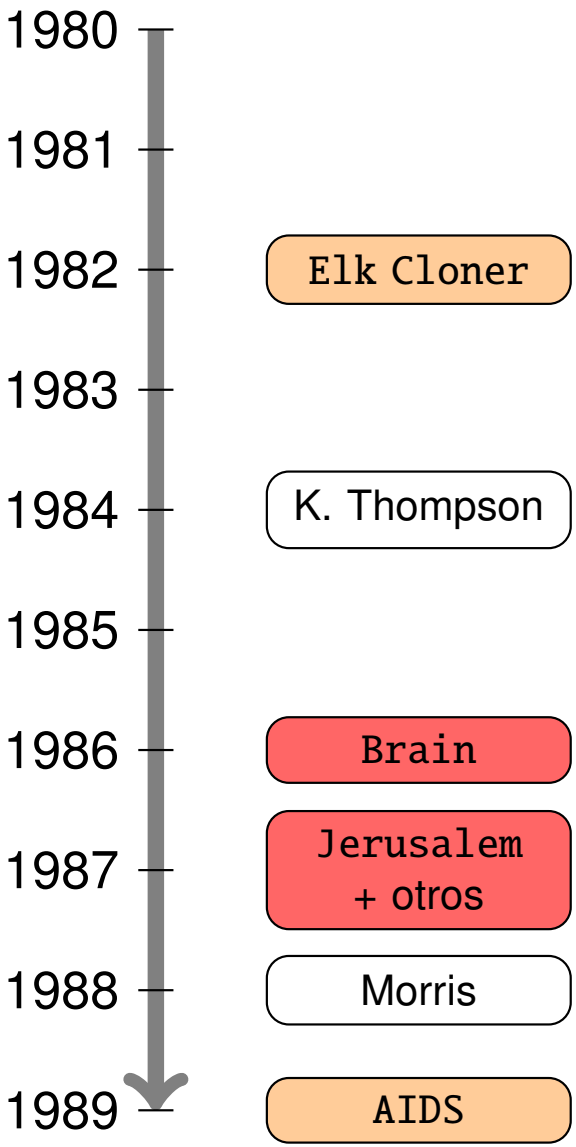




Evolución

Segunda etapa: 80s



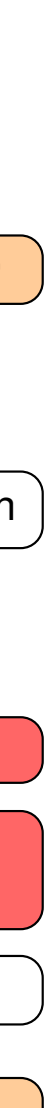


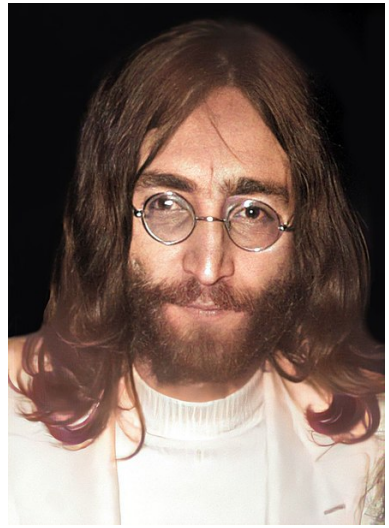
- `Elk Cloner` (Richard Skrenta)
- Ken Thompson
- `Brain` (Basit y Amjad Farooq Ali)
- `Jerusalem` y más virus de sector de arranque
- Gusano `Morris` (Robert T. Morris)
  - Sistemas DEC VAX/Sun3 con BSD
  - **Primera explotación de BOF** (en `fingerd`)
  - doi: 10.1145/66093.66095

Universidad Zaragoza

Evolución

Segunda etapa: 80s



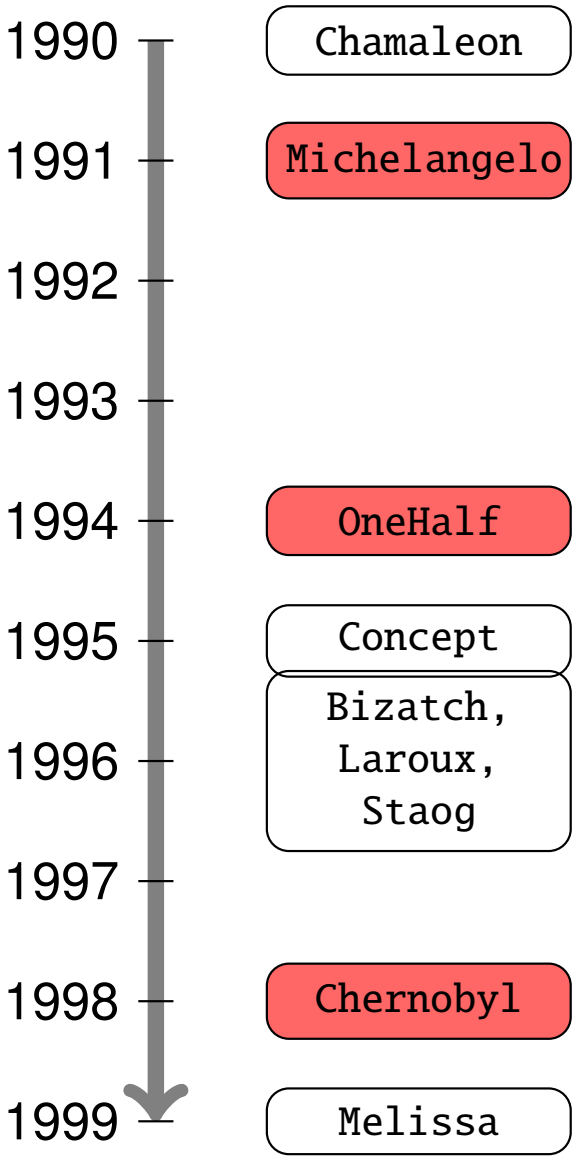


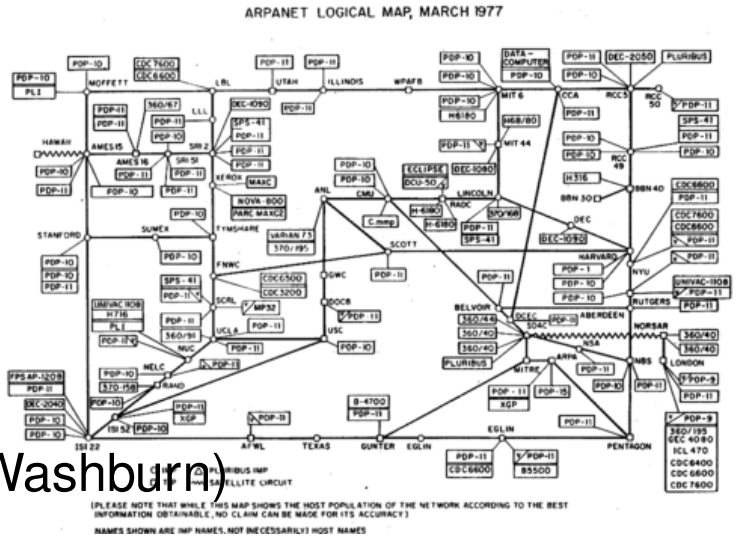
- `Elk Cloner` (Richard Skrenta)
- Ken Thompson
- `Brain` (Basit y Amjad Farooq Ali)
- `Jerusalem` y más virus de sector de arranque
- Gusano `Morris` (Robert T. Morris)
- `AIDS` (Dr. Joseph Popp)
  - Sistemas DOS
  - **Primer *ransomware*. Criptografía simétrica** 🙂
  - Análisis técnico: `https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf`

Universidad Zaragoza

Evolución

Tercera etapa: 90s

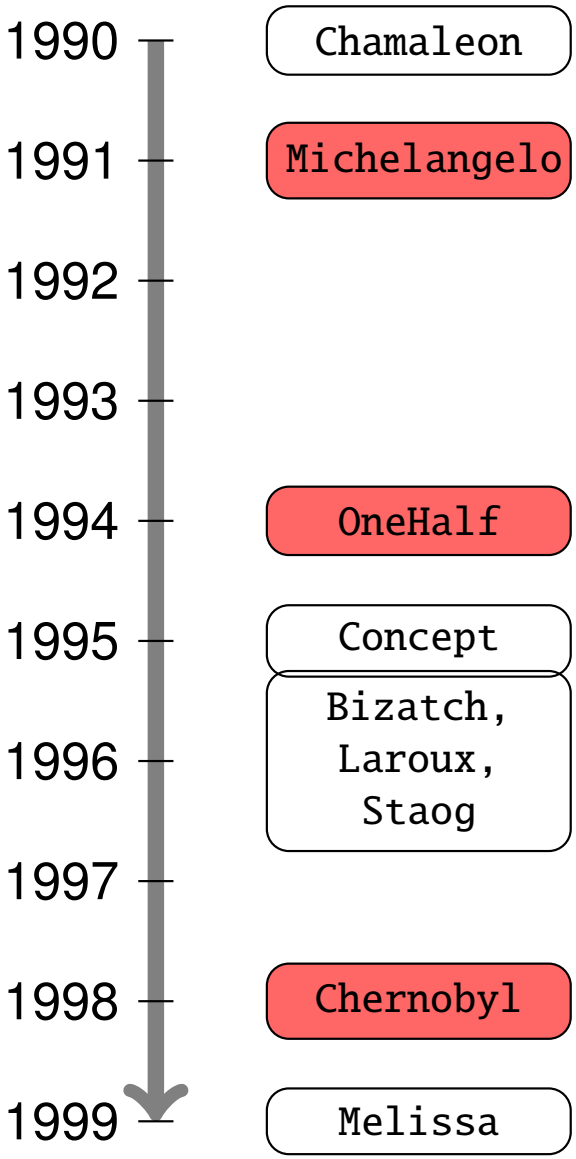


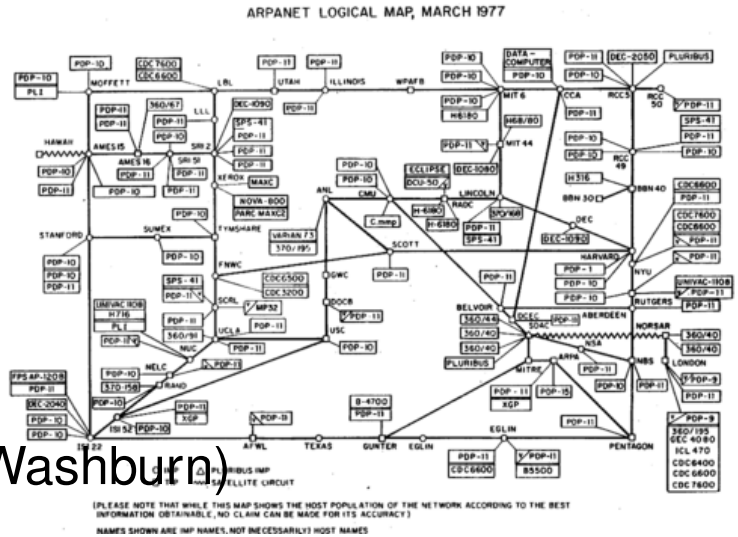


- Chamaleon (Mark Washburn)
  - Sistemas DOS
  - **Primer virus polimórfico**
    - Derivado del virus Vienna

Evolución

Tercera etapa: 90s

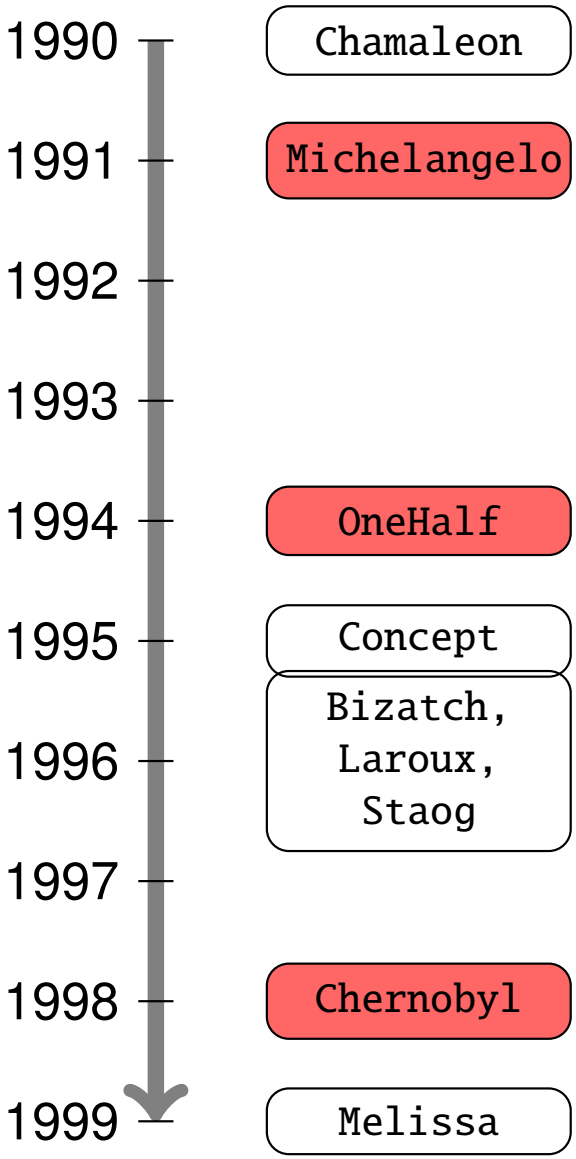


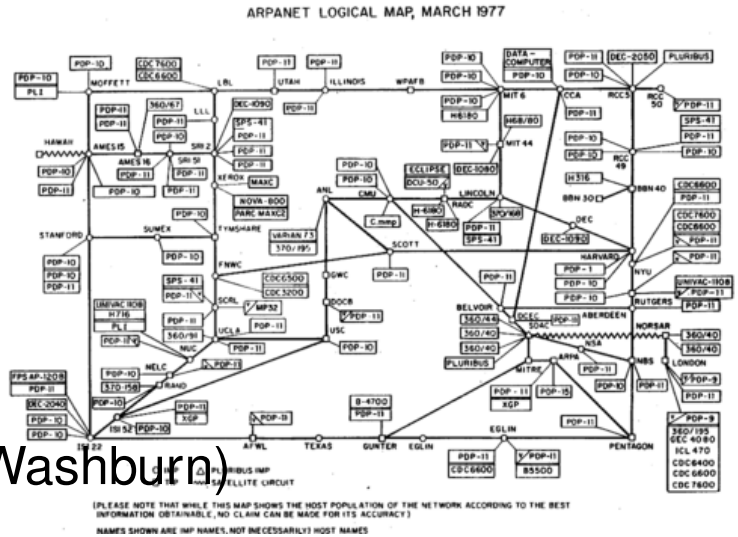


- Chamaleon (Mark Washburn)
- Michelangelo
  - Sistemas DOS
  - **Borrado de contenido el 6 de marzo**
  - **Mucha atención mediática**, pero sólo impactó unos 10K sistemas

Evolución

Tercera etapa: 90s

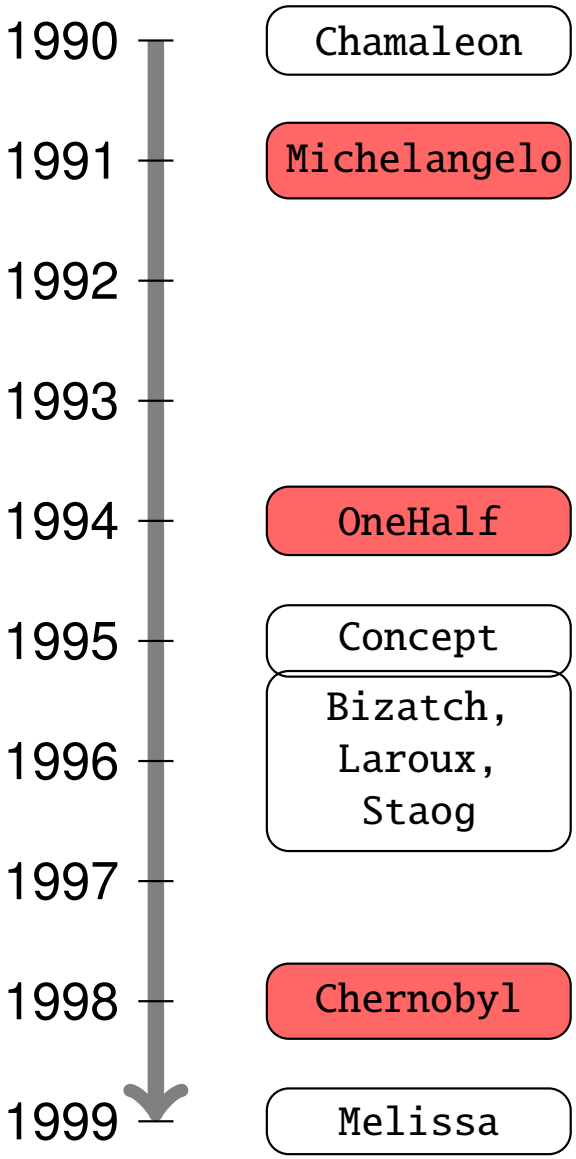


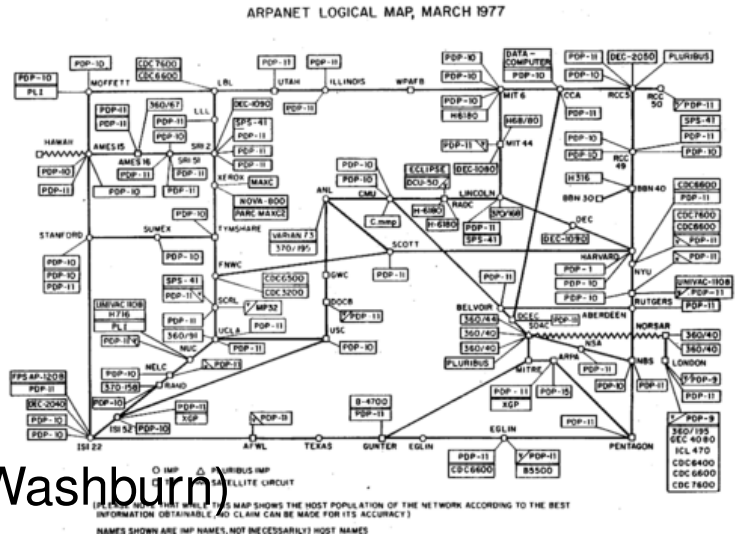


- Chamaleon (Mark Washburn)
- Michelangelo
- OneHalf
  - Sistemas DOS
  - **Infector dual: archivos y sector de arranque**
  - Acababa cifrando todo el disco si no se eliminaba a tiempo

Evolución

Tercera etapa: 90s

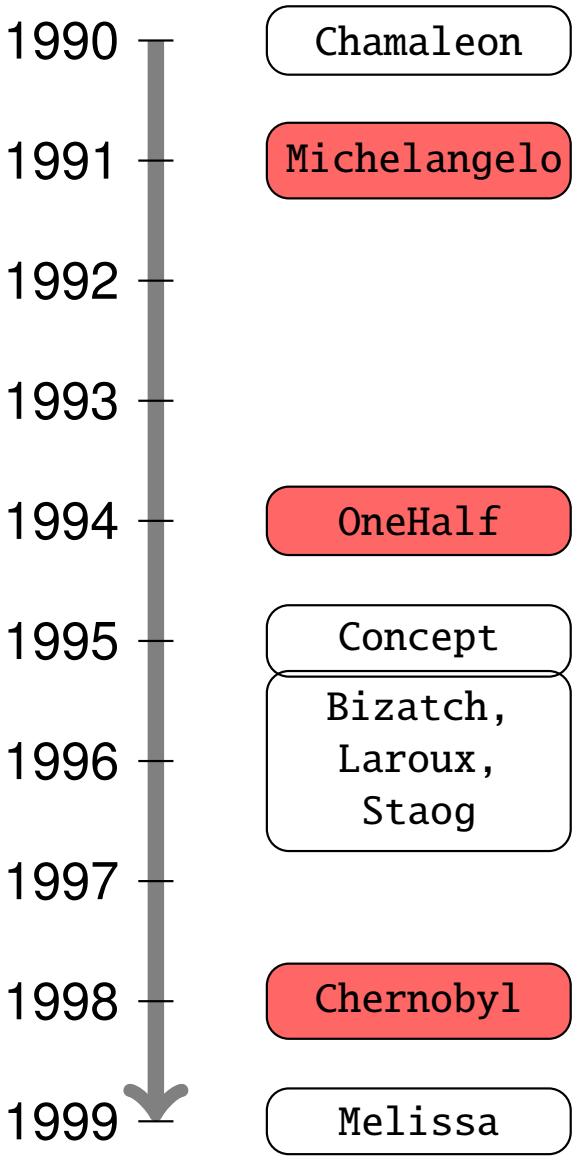


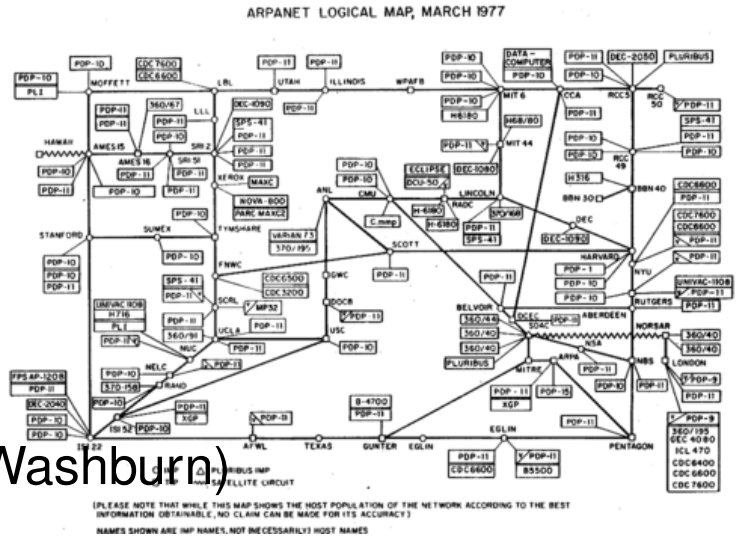


- Chamaleon (Mark Washburn)
- Michelangelo
- OneHalf
- Concept
  - Aplicación Microsoft Word 95 y Word 6.0 (multiplataforma)
  - **Primer virus de macros encontrado**
    - DMV fue antes (1994), pero era de laboratorio

Evolución

Tercera etapa: 90s

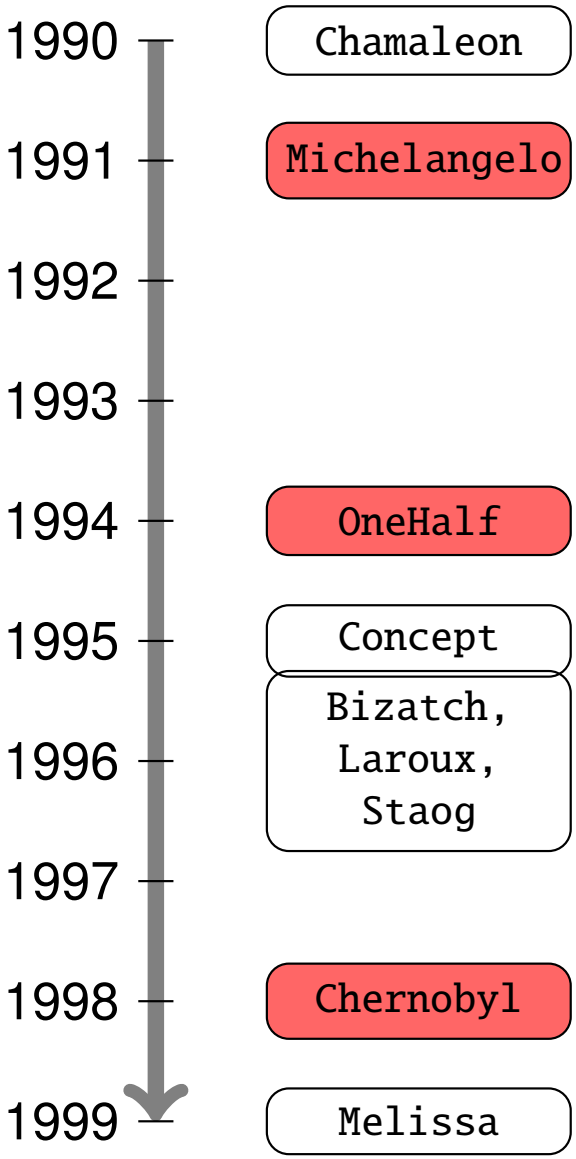


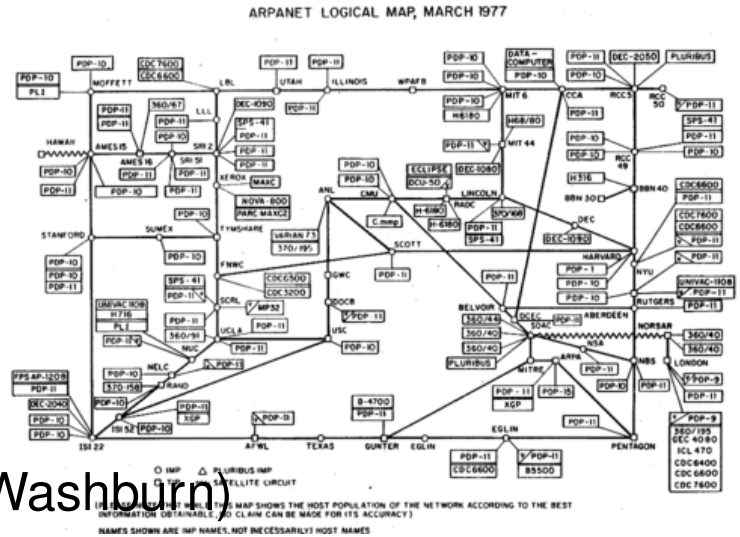


- Chamaleon (Mark Washburn)
- Michelangelo
- OneHalf
- Concept
- Bizatch, Laroux, Staog
  - Bizatch: **primer infector para Win95** (por VLAD).
  - Laroux: **primer virus de macros Excel** (sólo Windows)
  - Staog: **primer virus para Linux**. Explotación de vulns para escalada de privilegios local

Evolución

Tercera etapa: 90s

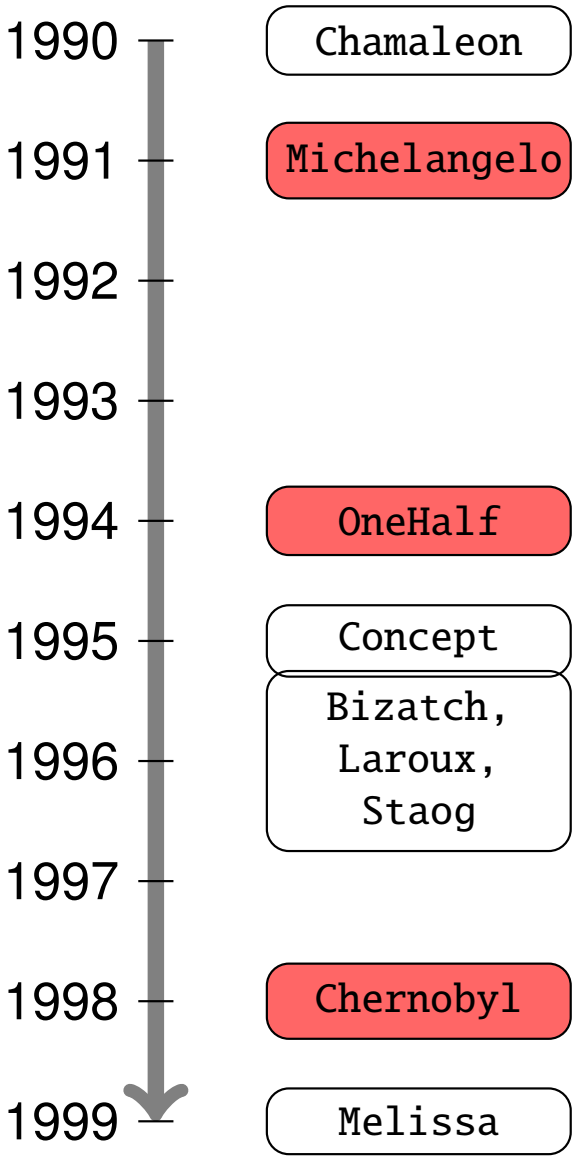


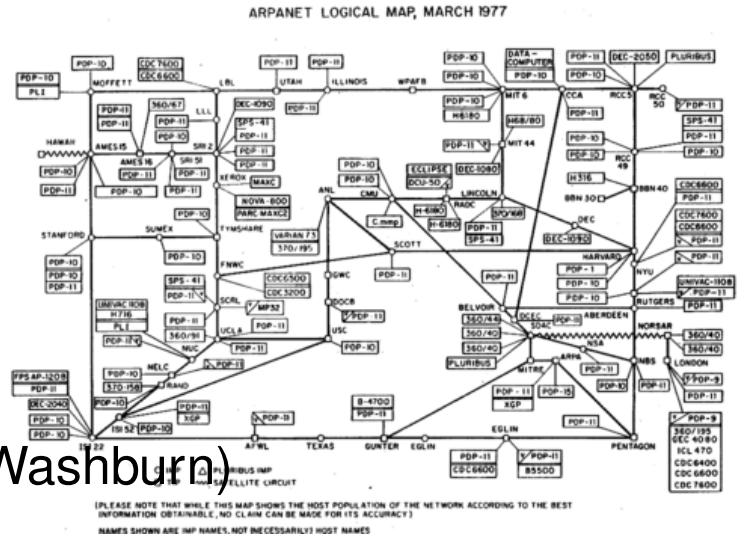


- Chamaleon (Mark Washburn)
- Michelangelo
- OneHalf
- Concept
- Bizatch, Laroux, Staog
- Chernobyl (Chen Ing Hau – CIH)
  - Sistemas Windows 95, 98 y ME. **Infector de ficheros**
  - Fecha de activación: 26 de abril
  - **Dos payloads**: sobrescritura del disco + Flash BIOS

Evolución

Tercera etapa: 90s





- Chamaleon (Mark Washburn)
- Michelangelo
- OneHalf
- Concept
- Bizatch, Laroux, Staog
- Chernobyl (Chen Ing Hau – CIH)
- Melissa
  - **Virus de macro** (Microsoft Word)
  - A través de Outlook, se distribuía a 50 contactos cada vez
  - **Causó denegación de servicio, aunque no era malicioso**

Universidad Zaragoza

Evolución

Cuarta etapa: inicios de los 2000s

2000 — ILOVEYOU, GTBot

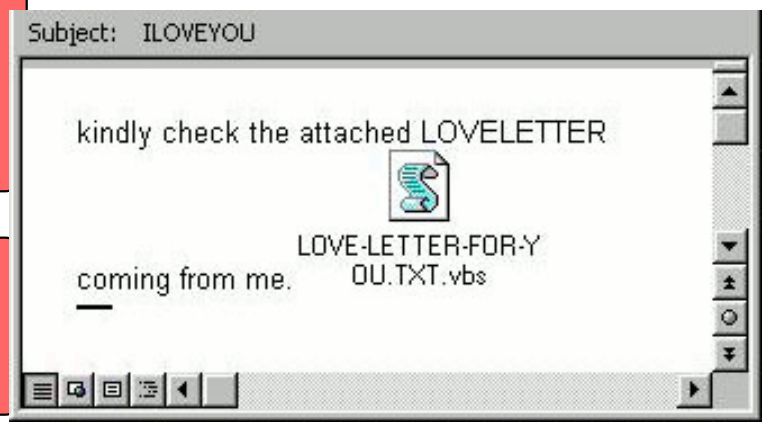
2001 — Kournikova, Sadmind, ...

2002 — MetaPHOR, MyLife ...

2003 — Sobig, Slammer, Spybot, Blaster, ...

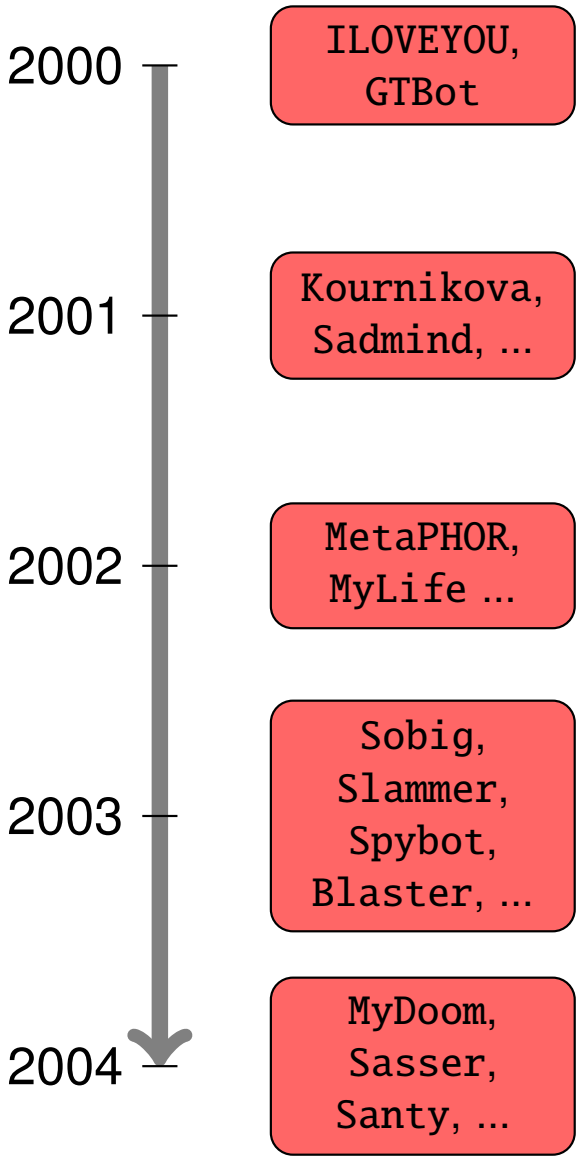
2004 — MyDoom, Sasser, Santy, ...

- ILOVEYOU, GTBot
  - ILOVEYOU
    - Sistemas Windows
    - **Difusión a través de mIRC y Outlook**
    - Modificación página inicial IE y ficheros
  - GTBot: primer bot IRC. DoS



Evolución

Cuarta etapa: inicios de los 2000s

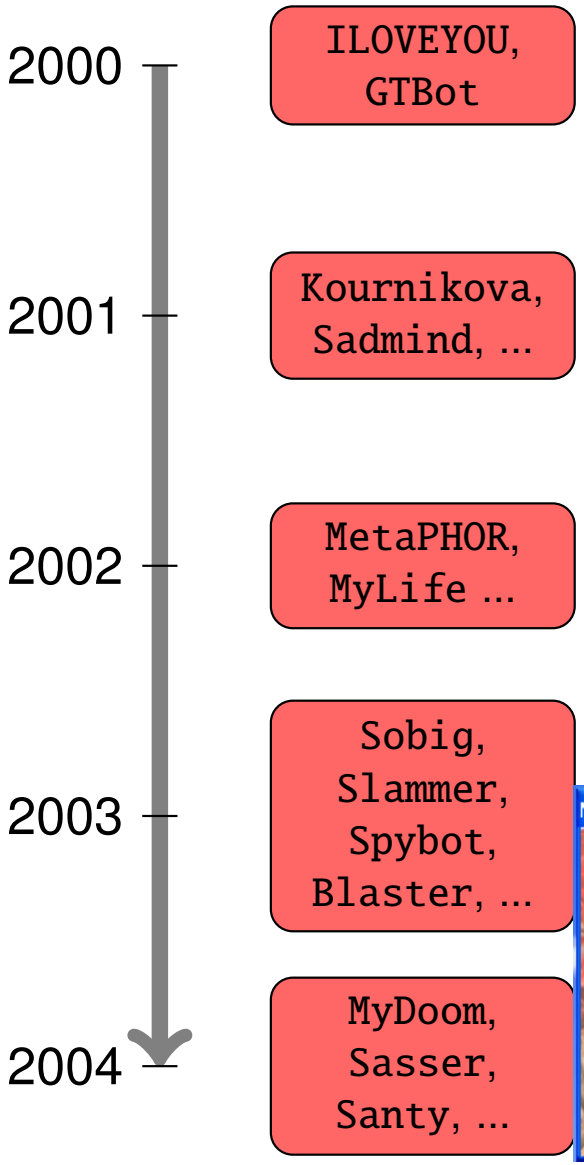


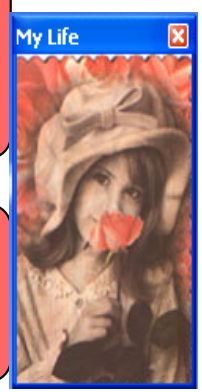
- ILOVEYOU, GTBot
- Anna Kournikova, Sadmind, etc.
  - Anna Kournikova: hecho con Kvbswg (Kalamar's VBS Worm Generator). DoS
  - Sadmin: gusano para Solaris, IIS (WinNT/2000). Defacing
  - Nimda: **primer gusano capaz de ejecutarse sin abrir el email**. Infección de ejecutables
  - CodeRed: gusano para IIS. Defacing
  - Klez: gusano destructivo, vía correo electrónico. Infección sin acción del usuario. Infección de ejecutables

Universidad Zaragoza

Evolución

Cuarta etapa: inicios de los 2000s



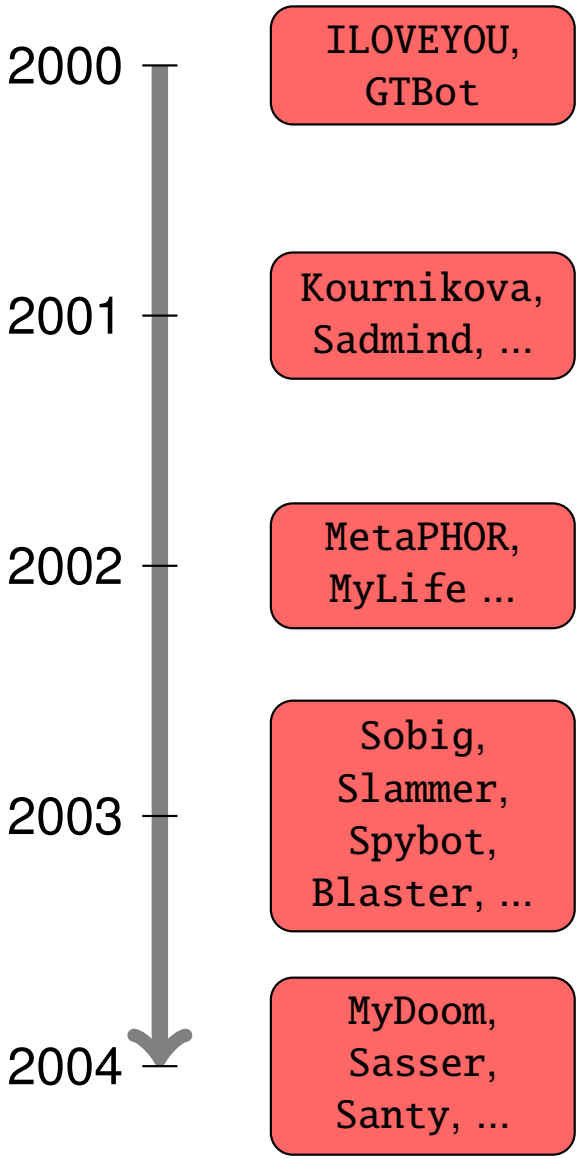


- ILOVEYOU, GTBot
- Anna Kournikova, Sadmind, etc.
- MetaPHOR, MyLife, Tanatos, etc.
  - MetaPHOR:
    - Sistemas Windows y Linux. PoC
    - **Virus metamórfico** (de 29A)
    - dsr.segfault.es/stuff/website-mirrors/29A/29a-6/29a-6.602
  - MyLife: gusano altamente destructivo. Sistemas Windows
  - Tanatos: **con backdoor y keylogger**. Impresión aleatoria. Sistemas Windows

Universidad Zaragoza

Evolución

Cuarta etapa: inicios de los 2000s

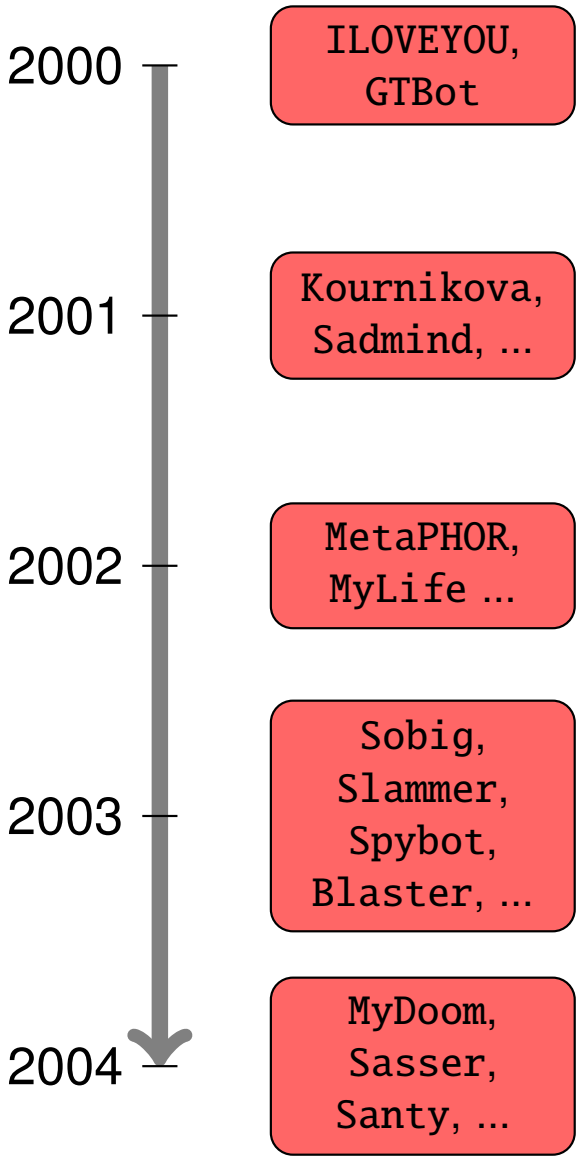


- ILOVEYOU, GTBot
- Anna Kournikova, Sadmind, etc.
- MetaPHOR, MyLife, Tanatos, etc.
- Sobig, Slammer, Spybot, Blaster, ...
  - Sobig: gusano email. Instala servidor Primer spammer
  - Slammer: Aplicación SQL Server (explotación BOF). Considerado primer gusano Warhol
  - Spybot: gusano P2P. C&C en IRC, con keylogger
  - Blaster: gusano TCP. Ataque DDoS
  - Welchia/Nachi: **gusano que elimina Blaster y parchea el sistema** (**nematodo**). No malicioso

Universidad Zaragoza

Evolución

Cuarta etapa: inicios de los 2000s

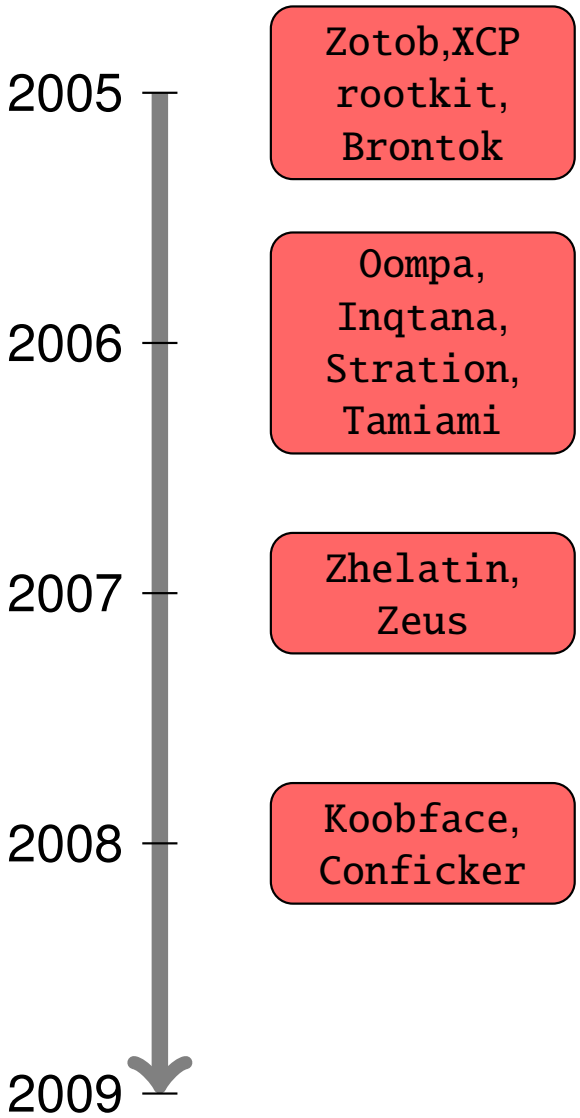


- ILOVEYOU, GTBot
- Anna Kournikova, Sadmind, etc.
- MetaPHOR, MyLife, Tanatos, etc.
- Sobig, Slammer, Spybot, Blaster, ...
- MyDoom, Sasser, Santy, ...
  - MyDoom: gusano email + P2P. DDoS
  - Sasser: gusano TCP. No malicioso (mucho DoS)
  - Santy: **primer gusano web**. Aplicación phpBB. Defacing
  - Witty: gusano UDP. **Primer gusano con alta difusión y destrucción**
  - Cabir: **gusano para Symbian OS**. MMS y Bluetooth

Universidad Zaragoza

Evolución

Cuarta etapa: finales de los 2000s

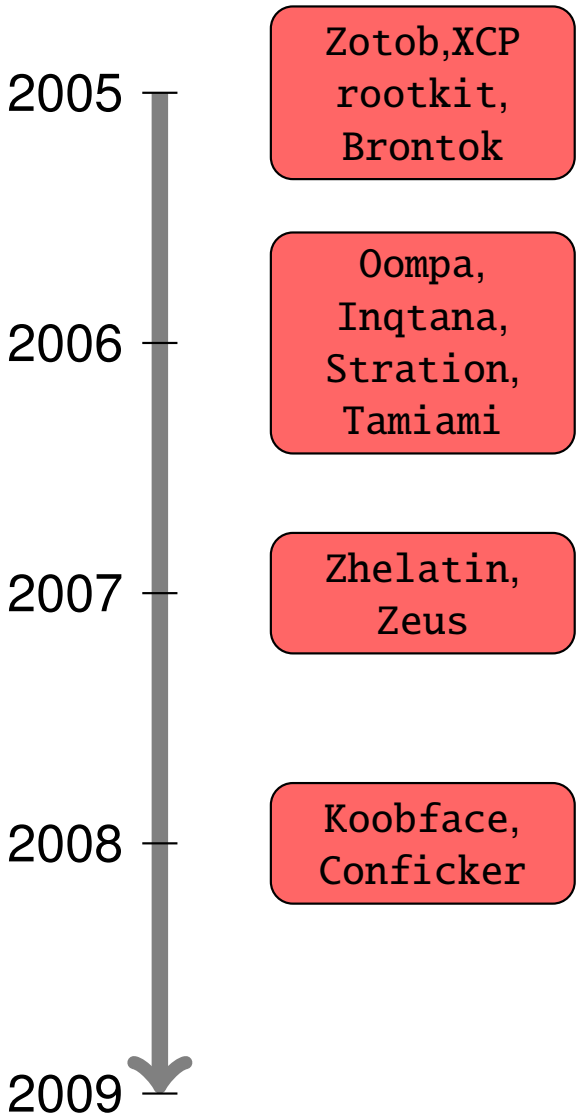


- Zotob, XCP rootkit, Brontok
  - Zotob: gusano TCP. Botnet
  - XCP rootkit
    - **Protección anti-copia DRM de Sony BMG**
    - Escándalo sonado. Más en este enlace
  - Brontok: gusano email. DoS webs específicas (PlayBoy, Israel)

Universidad Zaragoza

Evolución

Cuarta etapa: finales de los 2000s

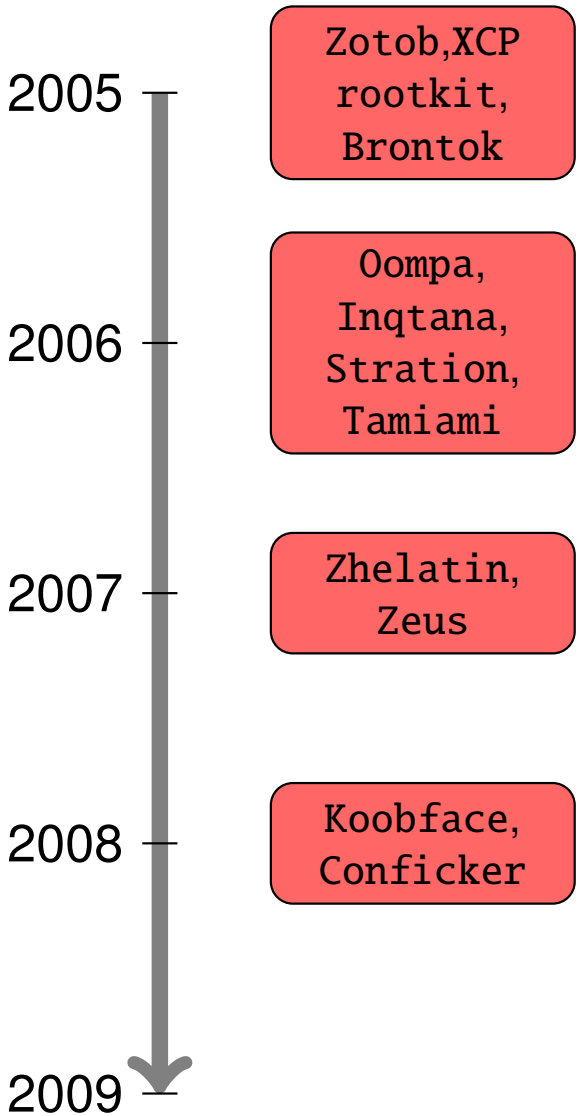


- `Zotob`, `XCP rootkit`, `Brontok`
- `Oompa`, `Inqtana`, `Stration`, `Tamiami`
  - `Oompa/Leap`: **primer gusano en macOS**. Aplicación iChat
  - `Inqtana`: otro gusano para macOS. PoC. Bluetooth
  - `Stration/Warezov`: gusano email. Botnet
  - `Tamiami`: gusano IRC/email. Infector

Universidad Zaragoza

Evolución

Cuarta etapa: finales de los 2000s

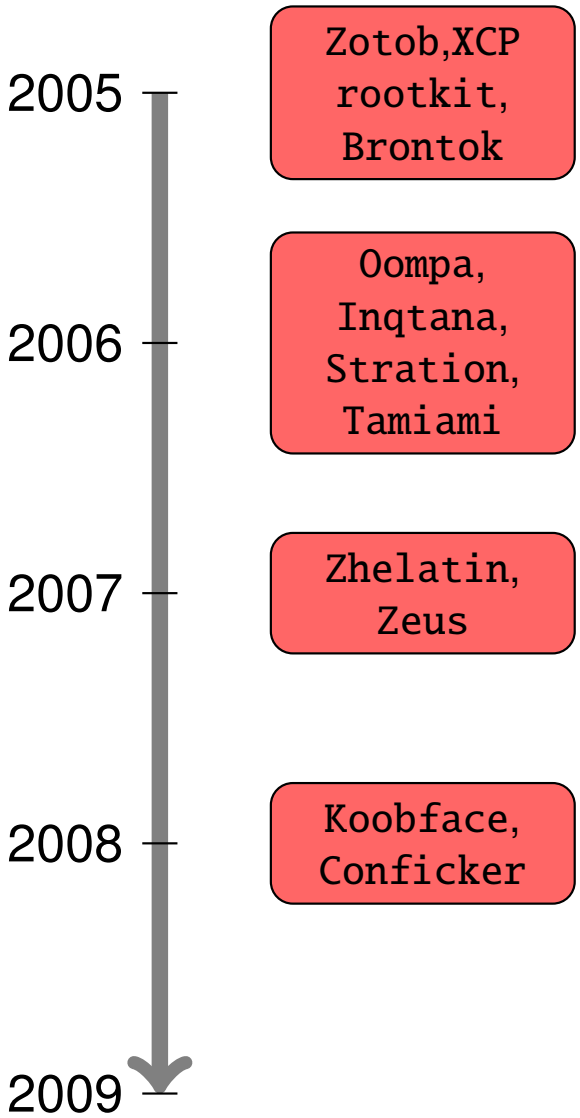


- Zotob, XCP rootkit, Brontok
- Oompa, Inqtana, Stration, Tamiami
- Zhelatin, Zeus
  - Zhelatin
    - Gusano email. Rootkit
    - **Origen del gusano Storm** (junto con Nuwar)
    - Botnet para envío de spam, keylogger
  - Zeus
    - **Troyano bancario avanzado**. Funciona hasta 2010
    - **PiTM keylogger en el navegador web**. También usado para distribuir otro malware
    - Propagación: drive-by-downloads, phising, scams

Universidad Zaragoza

Evolución

Cuarta etapa: finales de los 2000s

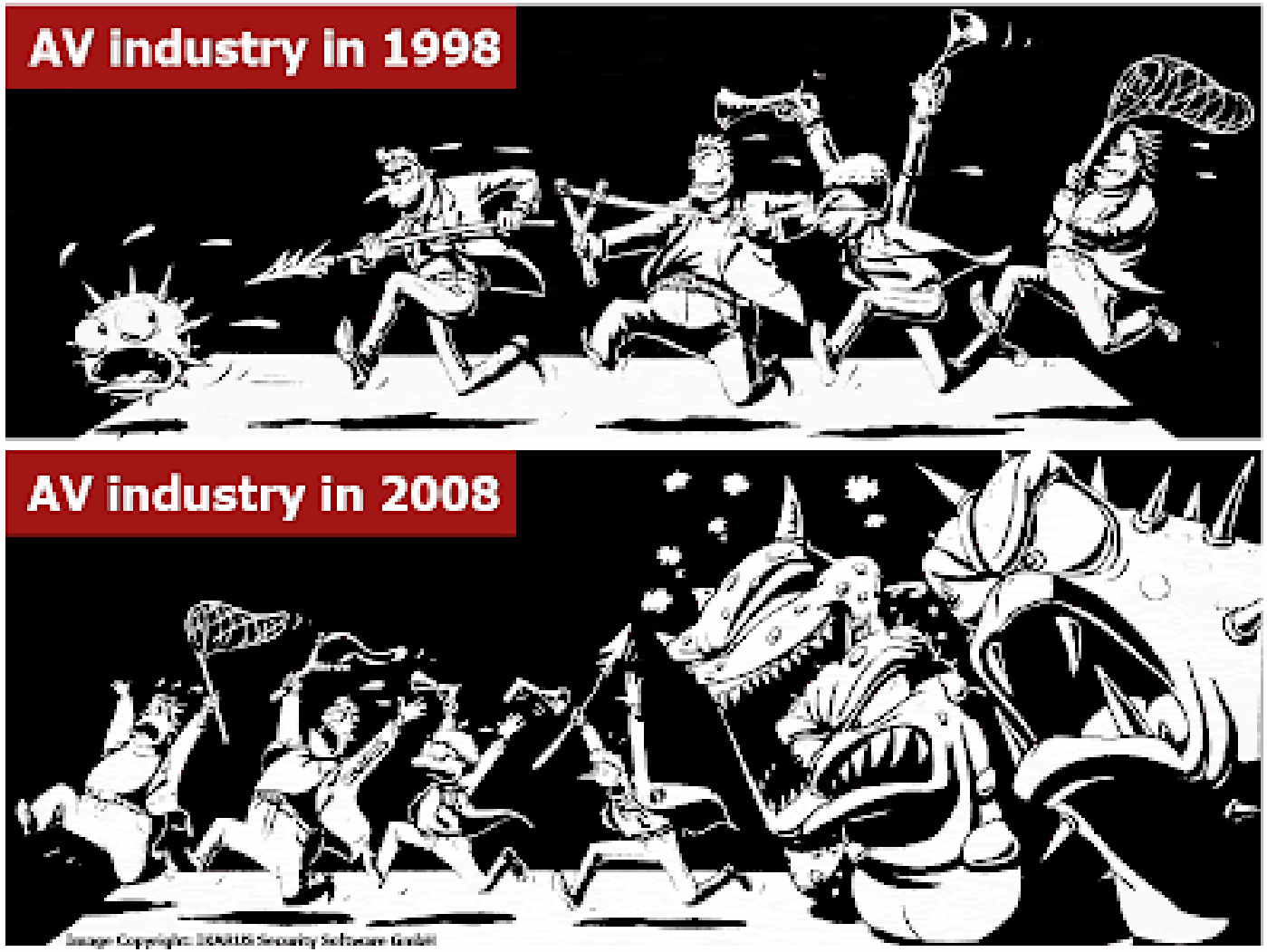


- Zotob, XCP rootkit, Brontok
- Oompa, Inqtana, Stration, Tamiami
- Zhelatin, Zeus
- Koobface, Conficker
  - Koobface: **gusano RRSS**. Keylogger
  - Conficker/Downadup/Kido
    - Gusano TCP. Explotación MS08-067
    - Botnet, file downloader

Universidad Zaragoza

Evolución

Quinta etapa: 2010 hasta la actualidad



Fuente: IKARUS Security Software

Evolución

Quinta etapa: 2010 hasta la actualidad

Cambio de tendencia: del lulz (kudos) por...

Universidad Zaragoza

Evolución

Quinta etapa: 2010 hasta la actualidad

Cambio de tendencia: del lulz (kudos) por...

Evolución

Quinta etapa: 2010 hasta la actualidad

Cambio de tendencia: del lulz (kudos) por...

`https://www.fbi.gov/wanted/cyber/`

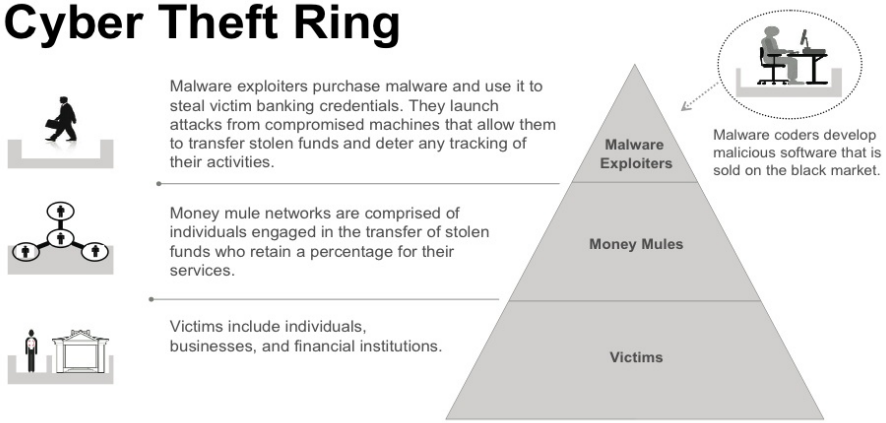
Algunos números...

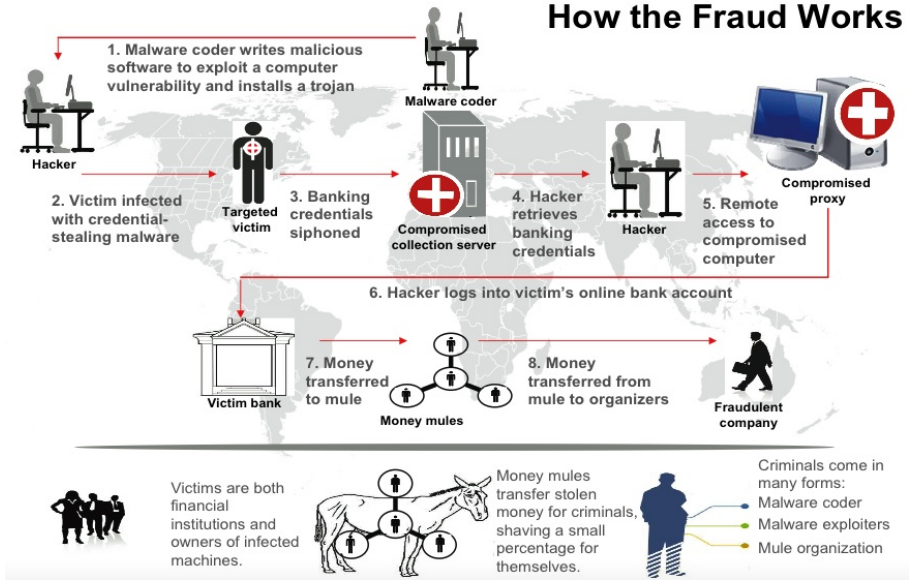
- `Zeus`: **más de $100M** (reconocidos)
- `Citadel`, `Dridex`: **se estiman unos £20M en UK, $10M en US** (**sólo 2015**)
  - O sea, unos £1.66M/mes, $833k/mes

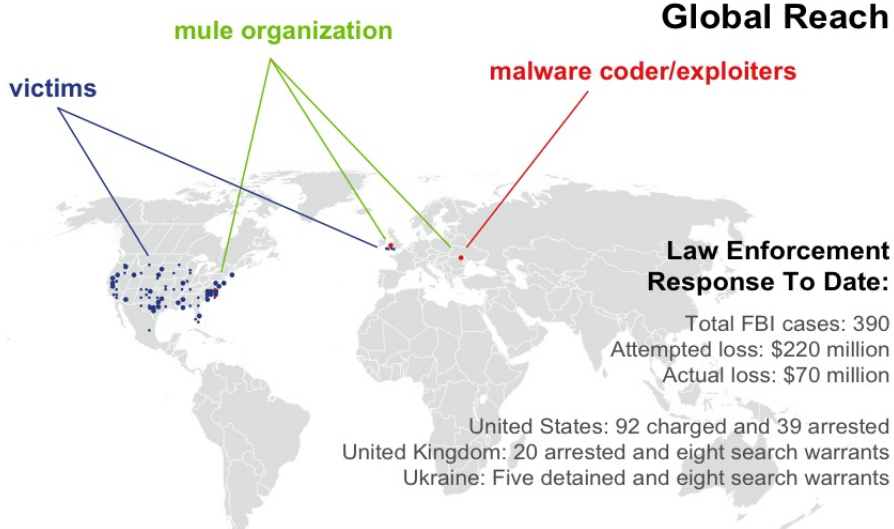
Universidad Zaragoza

Evolución

Quinta etapa: 2010 hasta la actualidad







Fuente: Wikipedia

Evolución

Quinta etapa: 2010 hasta la actualidad

Más tipos de malware

- **Porn diallers**
  - Viejos troyanos, de la época del módem
  - Cambio en/creación de configuración de conexión a teléfonos de tarificación especial

Evolución

Quinta etapa: 2010 hasta la actualidad

Más tipos de malware

- **Porn diallers**
  - Viejos troyanos, de la época del módem
  - Cambio en/creación de configuración de conexión a teléfonos de tarificación especial
- ***Advanced Persistent Threats*** (APT)
  - `Stuxnet` (2010)
    - **Primer malware de ICS**
    - **Vulnerabilidades de hardware usado en centrifugadoras de uranio** de Irán
    - **Cuatro 0-days**: CVE-2010-2568, -3888, -2743, y -2729
    - Atribuido a Israel-USA. *State-sponsored malware* (?)
  - `GhostNet`, `Duqu`, `Flame`, ...
  - **Lecturas de interés**:
    - "*The Real Story of Stuxnet*", D. Kushner, IEEE Spectrum, 2013
    - "*It's Time to Write the Rules of Cyberwar*", K. Rauscher, IEEE Spectrum, 2013
    - "*Stuxnet: Dissecting a Cyberwarfare Weapon*", R. Langner, IEEE S&P, 2011
    - Zero Days (2016) , `https://www.imdb.com/title/tt5446858/`

Universidad Zaragoza 1542

Evolución

Más tipos de malware

- **Spyware**
  - Robo de contraseñas, documentos, imágenes de cámara web, etc.
  - **Diferentes tipos**: *browser hijacking, keyloggers, clipboard hijacking*, etc.
  - Ejemplos: `CoolWebSearch`, `DarkHotel`

Universidad Zaragoza
1542

Evolución

Más tipos de malware

- **Spyware**
  - Robo de contraseñas, documentos, imágenes de cámara web, etc.
  - **Diferentes tipos**: *browser hijacking, keyloggers, clipboard hijacking*, etc.
  - Ejemplos: `CoolWebSearch`, `DarkHotel`
- **Software PUP** (*Potentially Unwanted Programs*; crapware)
  - **No son maliciosos, simplemente indeseados**
  - Ejemplos: adware

Universidad Zaragoza
1542

Evolución

Más tipos de malware

- **Spyware**
  - Robo de contraseñas, documentos, imágenes de cámara web, etc.
  - **Diferentes tipos**: *browser hijacking, keyloggers, clipboard hijacking*, etc.
  - Ejemplos: `CoolWebSearch`, `DarkHotel`
- **Software PUP** (*Potentially Unwanted Programs*; crapware)
  - **No son maliciosos, simplemente indeseados**
  - Ejemplos: adware
- **Rootkits**
  - **Diferentes tipos**: kernel-mode, bootkit, user-mode, virtual, firmware
  - Ejemplos: `Rkit`, `Aphex`, `Cloaker`, ...

Universidad Zaragoza

Evolución

Más tipos de malware

- **Ransomware**
  - Diferentes tipos: **crypto ransomware**, **locker ransomware**
  - Primer locker: `WinLock` (2011)
    - Conocidos también como *virus de la policía*
    - Bloquea acceso al sistema y pide rescate
    - Ejemplos: `Reveton`, `Ukash`, `Urausy`, `Kovter`
  - Primer crypto: `CryptoLocker` (2013). **Evolución explosiva**
    - Códigos fuente filtrados. "Facilidad" de implementación
    - Consejo: "*Don't roll your own crypto*"
    - Más famosos: `CryptoWall`, `CTB-Locker`, `Locky`, `WannaCry`, `Petya`, `Ryuk`
  - **Evolución a RaaS**: *Ransomware-as-a-Service*

Universidad Zaragoza

Evolución

Más tipos de malware

- **Ransomware**
  - Diferentes tipos: **crypto ransomware**, **locker ransomware**
  - Primer locker: `WinLock` (2011)
    - Conocidos también como *virus de la policía*
    - Bloquea acceso al sistema y pide rescate
    - Ejemplos: `Reveton`, `Ukash`, `Urausy`, `Kovter`
  - Primer crypto: `CryptoLocker` (2013). **Evolución explosiva**
    - Códigos fuente filtrados. "Facilidad" de implementación
    - Consejo: "*Don't roll your own crypto*"
    - Más famosos: `CryptoWall`, `CTB-Locker`, `Locky`, `WannaCry`, `Petya`, `Ryuk`
  - **Evolución a RaaS**: *Ransomware-as-a-Service*
- **POS RAM scrapper**
  - Analizan memoria RAM del sistema buscando tarjetas de crédito/débito
  - Primer familia conocida: `rdasvr` (2010)
  - Más problemático en USA, por su forma de funcionar
  - Lectura: "*Evolution and Characterization of Point-of-Sale RAM Scraping Malware*", R. J. Rodríguez, Journal in Computer Virology and Hacking Techniques, 2017, doi: 10.1007/s11416-016-0280-4

```
((b|B)[0-9]{13,19}\^[A-Za-z\s]{0,30}\/[A-Za-z\s]{0,30}\^(1[1-9])((0[1-9])|(1[0-2]))[0-9\s]{3,50}[0-9]{1})
([3-9]{1}[0-9]{14,15}[D=](1[1-9])((0[1-9])|(1[0-2]))[0-9]{8,30})
```

Evolución

Estimación de beneficios (2011)

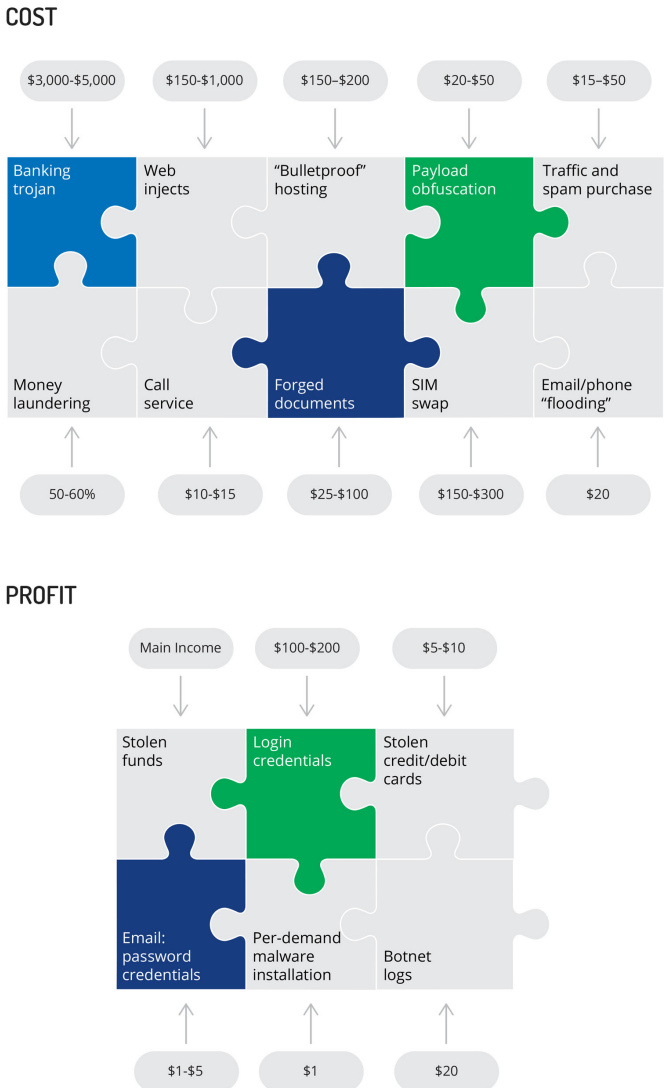
TREND	TOTAL MARKET SHARE	AMOUNT
ONLINE FRAUD		
Online banking fraud	21.3 %	490 million $
Cashing	16 %	367 million $
Phishing	2.4 %	55 million $
Theft of electronic funds	1.3 %	30 million $
Total:	41 %	942 million $
SPAM		
Spam	24 %	553 million $
Pharma and counterfeits	6.2 %	142 million $
Fake software	5.9 %	135 million $
Total:	36.1 %	830 million $
INTERNAL MARKET (C2C)		
Sale of traffic	6.6 %	153 million $
Sale of exploits	1.8 %	41 million $
Sale of loaders	1.2 %	27 million $
Anonymization	0.4 %	9 million $
Total:	10 %	230 million $
DDOS ATTACKS		
DDoS attacks	5.6 %	130 million $
Total:	5.6 %	130 million $
OTHER		
Other	7.3 %	168 million $
Total:	7.3 %	168 million $

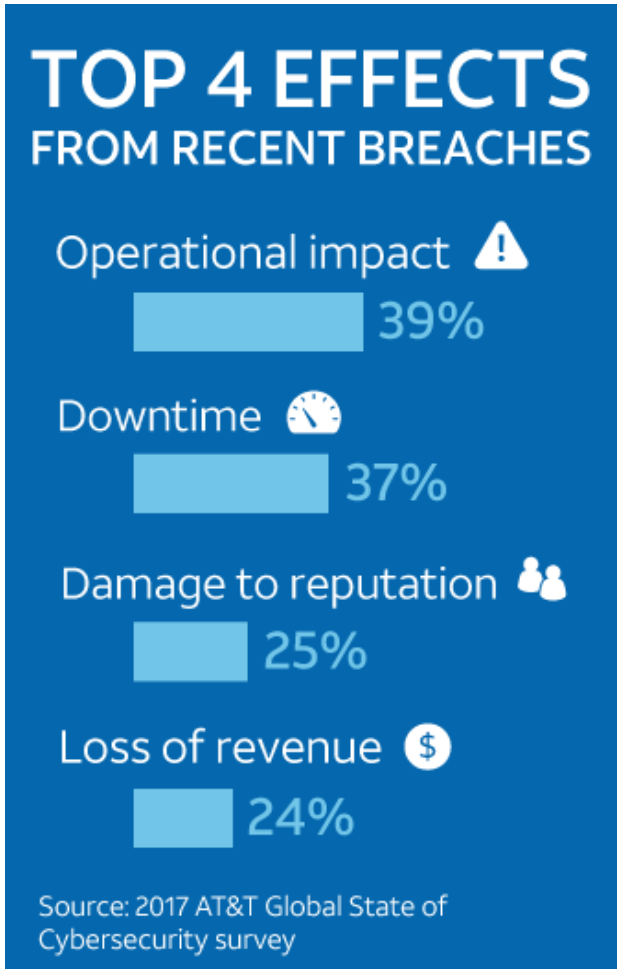
- En 2013, **3 trillones de dólares** (según Europol)
  - **Más rentable que el mercado conjunto de la marihuana, cocaína y heroína**
  - `https://www.europol.europa.eu/sites/default/files/documents/socta2013.pdf`

Fuente: `http://www.securityaffairs.co/`

Evolución

Estimación de beneficios (2017)

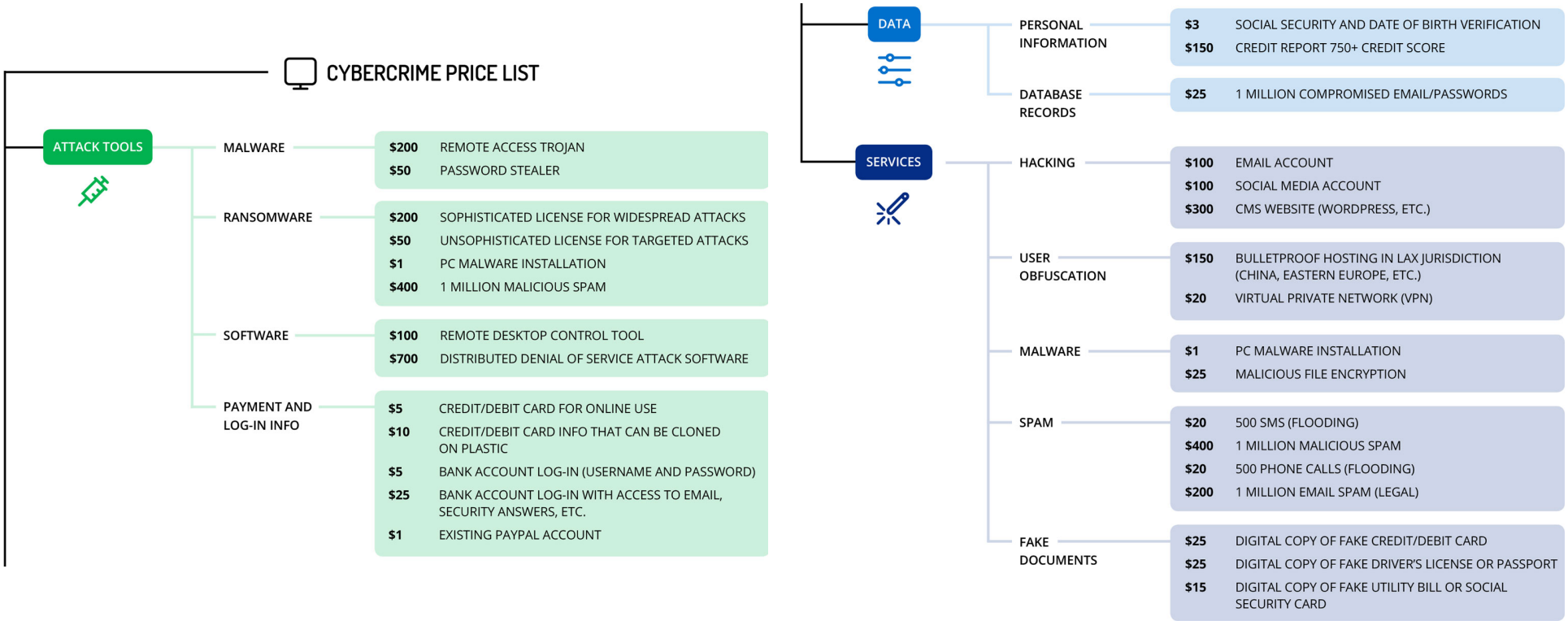




Fuente: `https://www.recordedfuture.com/cyber-operations-cost/`

Evolución

¡Vámonos de compras! (2017)



Fuente: `https://www.recordedfuture.com/cyber-operations-cost/`

Universidad Zaragoza 1542

Índice

Universidad Zaragoza

Análisis de malware

Metodología de análisis de malware 101

Análisis estático (código muerto, código en frío)

- **Firmas hash** (MD5, SHA1, SHA-256)
  - Búsqueda en servicios como VT o Google
  - *¿Hay ya algún análisis previo o clasificación por AVs?*
- **Cadenas contenidas en el fichero**: `strings`
- **Propiedades del fichero PE** (*¿está protegido?*)
  - Verificar las funciones importadas (no es concluyente, pero puede dar indicios sobre su actividad)

Universidad Zaragoza

Análisis de malware

Metodología de análisis de malware 101

Análisis dinámico (código vivo, código en caliente)

- Normalmente, en máquina virtual o aislada
- **Interacción con el SO: ficheros**
  - ¿Creación? ¿Acceso? ¿Modificación? ¿Eliminación?
- **Interacción con el SO: Registro de Windows**
  - ¿Creación? ¿Acceso? ¿Modificación? ¿Eliminación?
- **Interacción con el SO: procesos**
  - ¿Creación? ¿Acceso?
- **Interacción con el exterior: comunicaciones de red**
  - Dirección IP
  - Nombres de dominio

Universidad Zaragoza
1542

Análisis de malware

Metodología de análisis de malware 101

Análisis dinámico (código vivo, código en caliente)

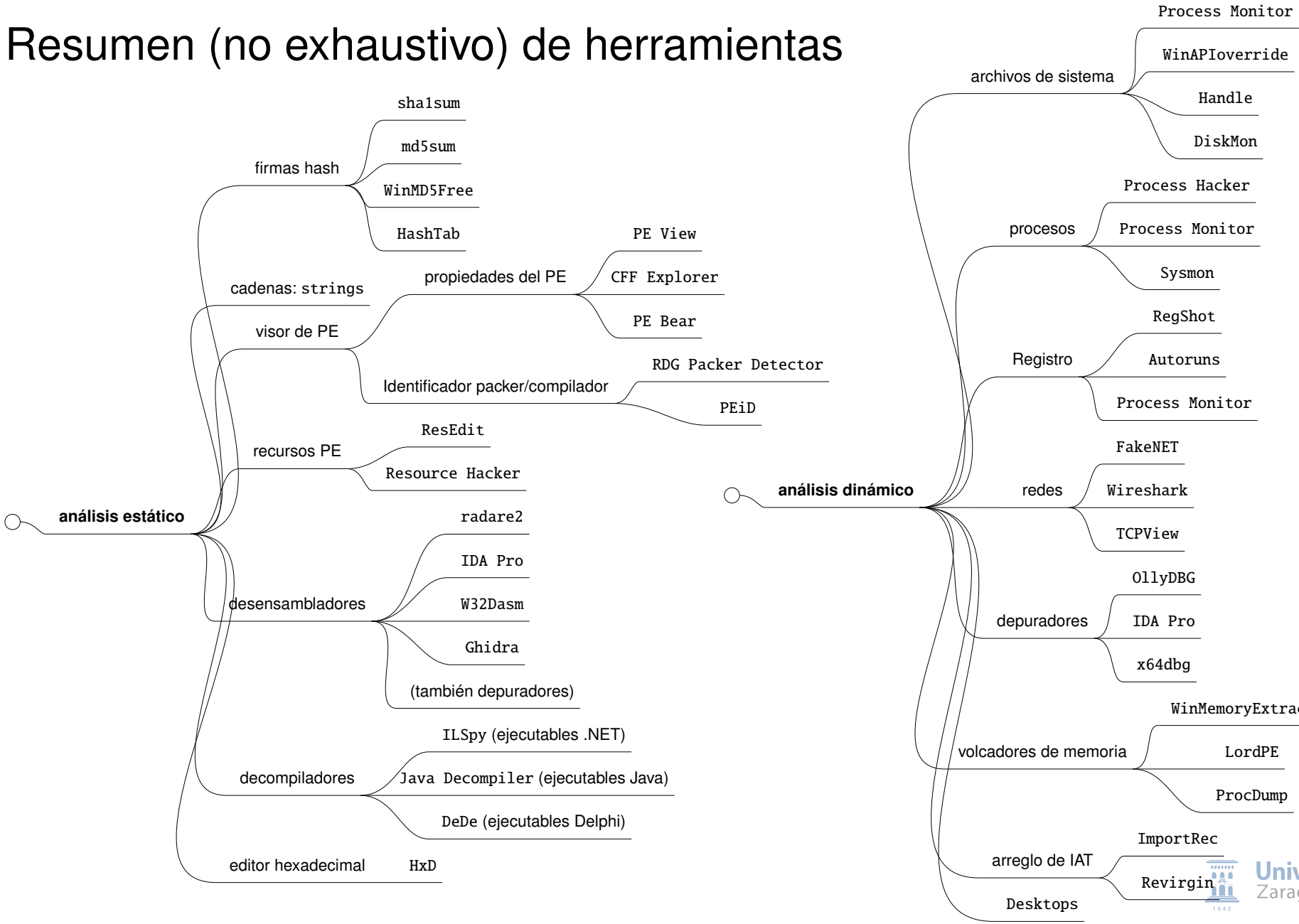
- Normalmente, en máquina virtual o aislada
- **Interacción con el SO: ficheros**
  - ¿Creación? ¿Acceso? ¿Modificación? ¿Eliminación?
- **Interacción con el SO: Registro de Windows**
  - ¿Creación? ¿Acceso? ¿Modificación? ¿Eliminación?
- **Interacción con el SO: procesos**
  - ¿Creación? ¿Acceso?
- **Interacción con el exterior: comunicaciones de red**
  - Dirección IP
  - Nombres de dominio

Averiguar el patrón del comportamiento

Universidad Zaragoza
1542

Análisis de malware

Resumen (no exhaustivo) de herramientas



Análisis de malware

DEMO

Universidad Zaragoza

Índice

Universidad Zaragoza

¿Hacia dónde vamos?

1. **Nuevas plataformas**:
   - **Entornos móviles**
   - **Entornos IoT**
   - **Entornos industriales conectados**

Universidad Zaragoza

¿Hacia dónde vamos?

1. **Nuevas plataformas**:
   - **Entornos móviles**
   - **Entornos IoT**
   - **Entornos industriales conectados**
2. **Evolución de malware**:
   - **Reaparición de viejos métodos en nuevas plataformas**
   - **Malware empacado/ofuscado**
   - **Malware consciente** (se protege)

Universidad Zaragoza

¿Hacia dónde vamos?

1. **Nuevas plataformas**:
   - **Entornos móviles**
   - **Entornos IoT**
   - **Entornos industriales conectados**
2. **Evolución de malware**:
   - **Reaparición de viejos métodos en nuevas plataformas**
   - **Malware empacado/ofuscado**
   - **Malware consciente** (se protege)
3. **Investigación de malware**
   - Cerca de dos décadas
   - **Problemas de reproducibilidad**
   - **Necesidad de más investigación ofensiva**
   - **Necesidad de ajustar datasets a entornos reales**
   - Lectura de (mucho) interés: "*Challenges and pitfalls in malware research*", M. Botacin et al., Computers & Security, 2021, doi: 10.1016/j.cose.2021.102287

Universidad Zaragoza
1542

Índice

Universidad Zaragoza

Bibliografía

- **The Virus Encyclopedia**, `http://virus.wikidot.com/`
- **Códigos fuentes en GitHub**, `https://github.com/yorickdewid/`
- **Malware Zoo,** `https://thezoo.morirt.com`
- Libros de interés:
  - *Practical reverse engineering : x86, x64, ARM, Windows Kernel, reversing tools, and obfuscation* / Bruce Dang, Alexandre Gazet, Elias Bachaalany ; with contributions from Sebastien Josse. Indianapolis, IN: John Wiley and Sons, 2014
  - *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard. John Wiley & Sons, Sep 29, 2010
  - *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, Michael Sikorski, Andrew Honig, No Starch Press, 2012

Universidad Zaragoza
1542

50 años conviviendo con los virus informáticos: *Una breve historia del malware*

Ricardo J. Rodríguez

rjrodriguez@unizar.es ※ @RicardoJRdez ※ www.ricardojrodriguez.es

Universidad Zaragoza

Dpto. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza, España

23 de julio, 2021

RetroEuskal
(online)