Historia del Malware

Ing. Pablo Frias

McAfee™ by Intel

TECH DAY
SEGUNDA EDICIÓN

After Office para desarrolladores y techies

- Charla técnica en simultáneo
  Los juegos de azar, uno de los tópicos más importantes del conocimiento humano • Machine Learning
- Demos de Mc Afee by Intel y empresas invitadas
- Sorteos
- Chips 'n Drinks ☺

JUEVES 30 DE MARZO
18:30 a 21:30

CIUDAD EMPRESARIA
EDIFICIO MIRAGOLF
Av. La Voz del Interior 7000
3ER PISO

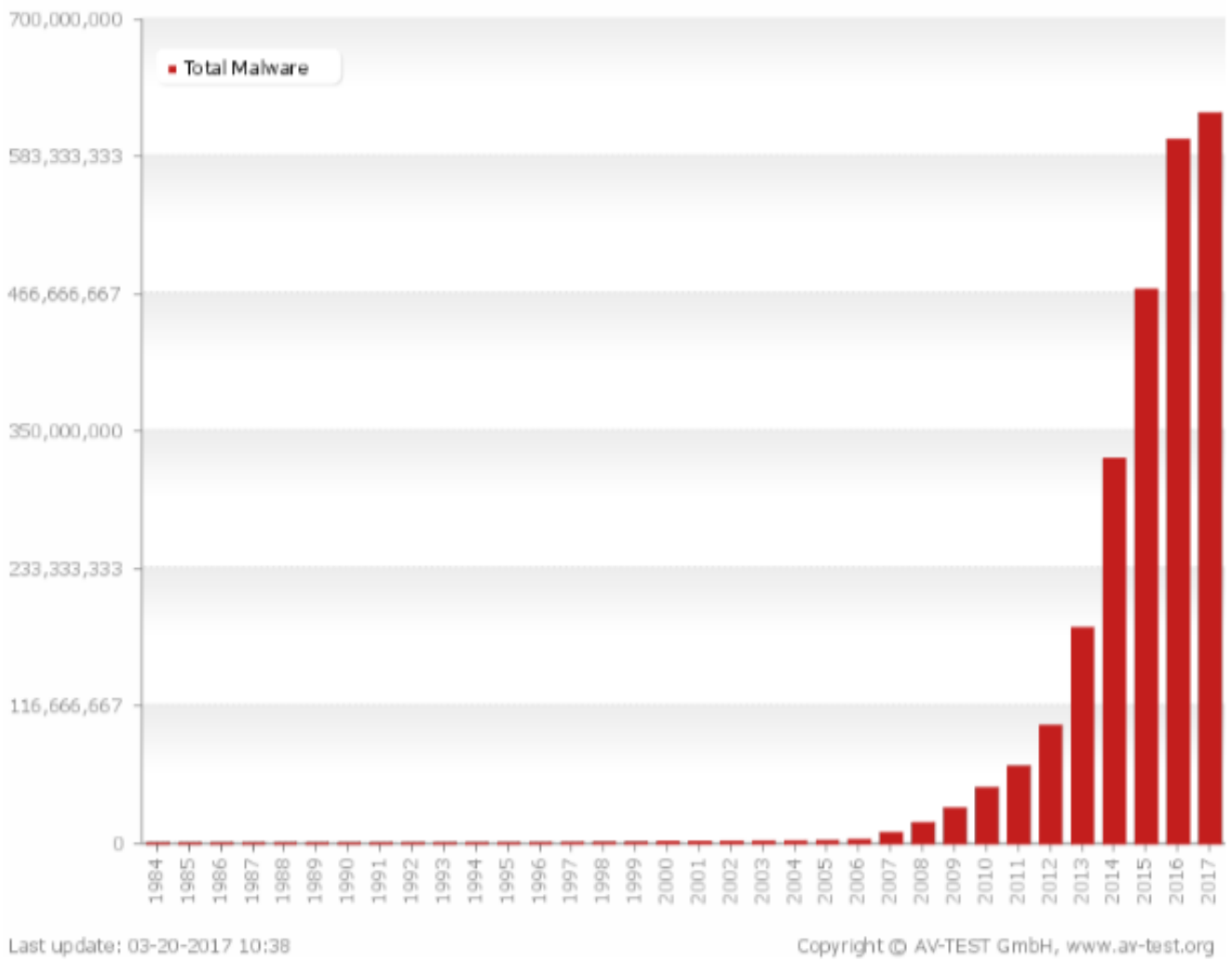
Inscribite en: https://techdaymcafeebyintel.eventbrite.es • Cupos limitados!

Participan

ASC ASCENTIO TECHNOLOGIES · IGS · LB-DataSecurity · Olapic · VOLT motors

Cuántos?

- Se registran 390.000 programas maliciosos por día.



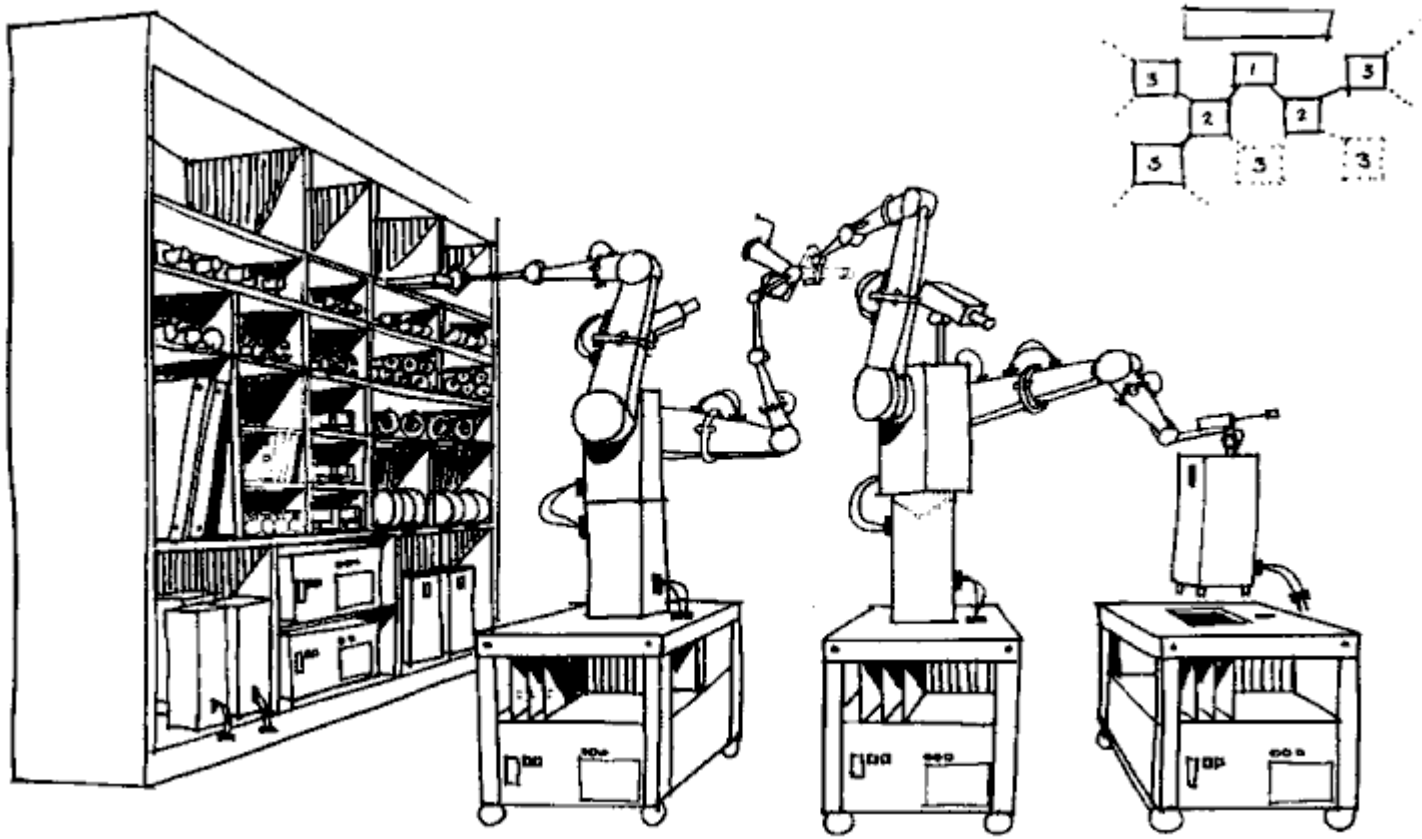
McAfee™ by Intel

Dónde comenzó todo

- 1949 - John von Neumann "Theory of self-reproducing automata"

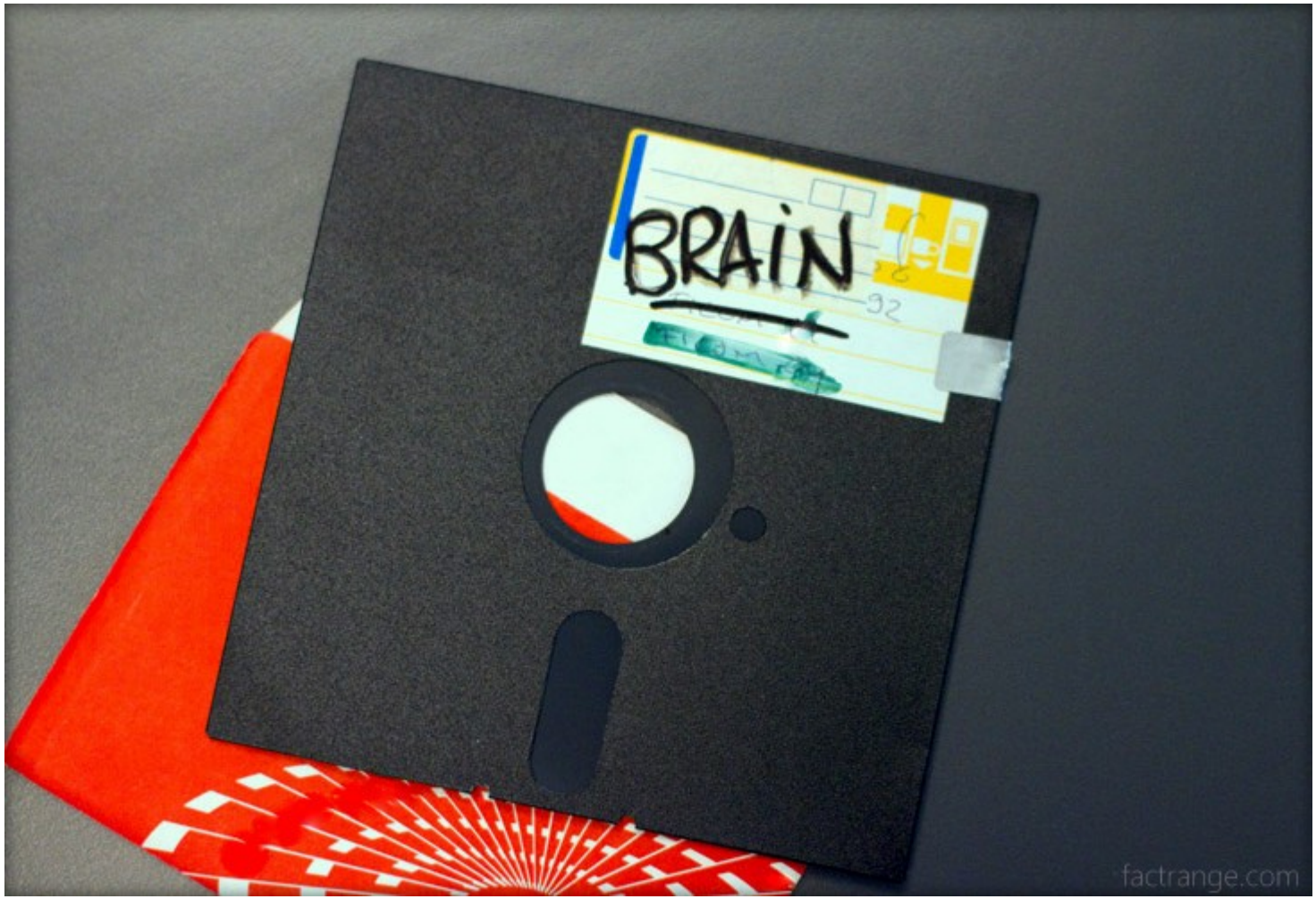
McAfee by Intel

Self-reproducing automata



McAfee by Intel

1986



McAfee by Intel

1986 - Brain

- Creado por Basit y Alvi Amjad (Pakistán)

McAfee by Intel

1986 - Brain

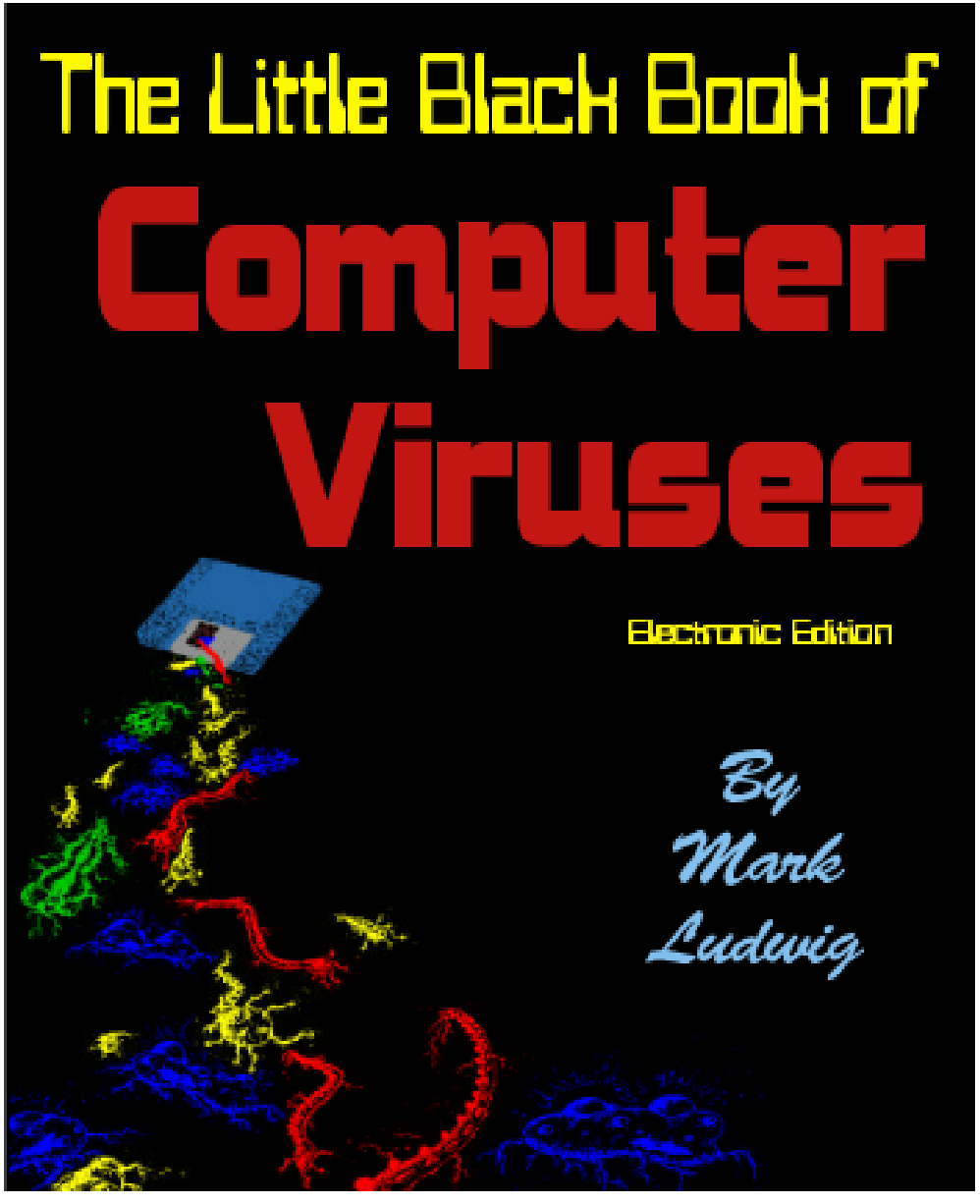
- Plataforma: MS-DOS
- Vector: discos de 5.25
- Técnica: Stealth
- Se alojaba en el sector de booteo del diskette.

McAfee by Intel

Técnica Stealth

- Oculta las modificaciones de tamaño de archivo para no ser detectado.
- Interfiere las llamadas de sistema para “forzar” los resultados.
- Brain monitoreaba el I/O del disco para redirigir las lecturas del boot sector infectado al espacio de memoria original.

1990 Mark Ludwig



- Se puede bajar de internet!

McAfee by Intel

1991 - Michelangelo

YOUR LEISURE READING

Michelangelo virus attacks P.C. data worldwide

Japan

Widespread

1991 - Michelangelo

- Plataforma: MS-DOS
- Vector: diskettes
- Técnica: Stealth
- Se alojaba en el sector de booteo del disco y operaba a nivel de BIOS.
- Sólo se activaba los dias 6 de Marzo.
- Modificaba los primeros 100 sectores del disco duro con nulls.
- Nunca se conoció su autor.

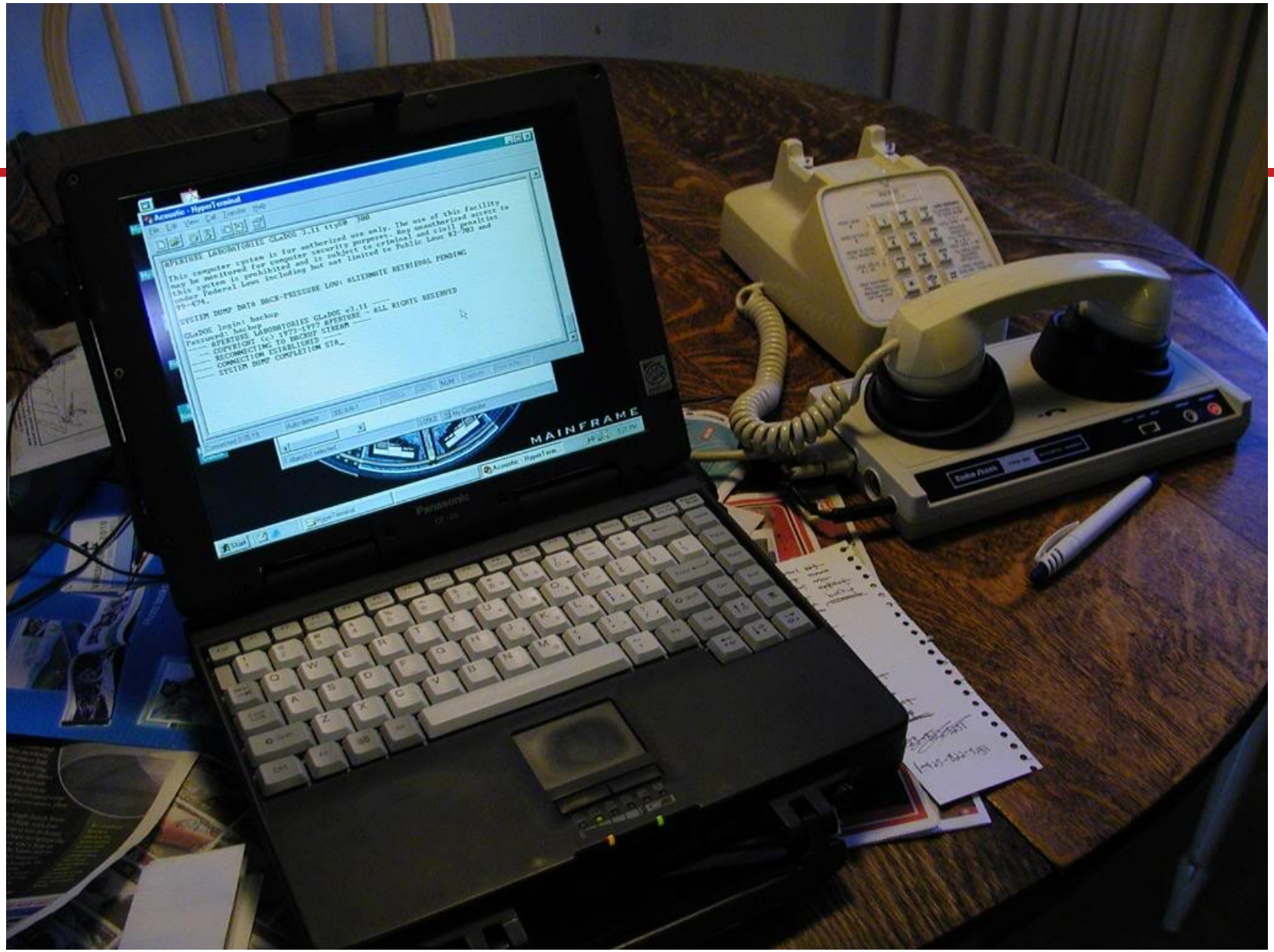
1993 - Leandro

- Plataforma: MS-DOS / Win 95/98
- Vector: diskettes
- MBR virus
- Activado los 21 de Octubre
- Escrito en ASM x86-16 bit
- 1024 bytes

McAfee by Intel

Vector de transmisión

McAfee by Intel

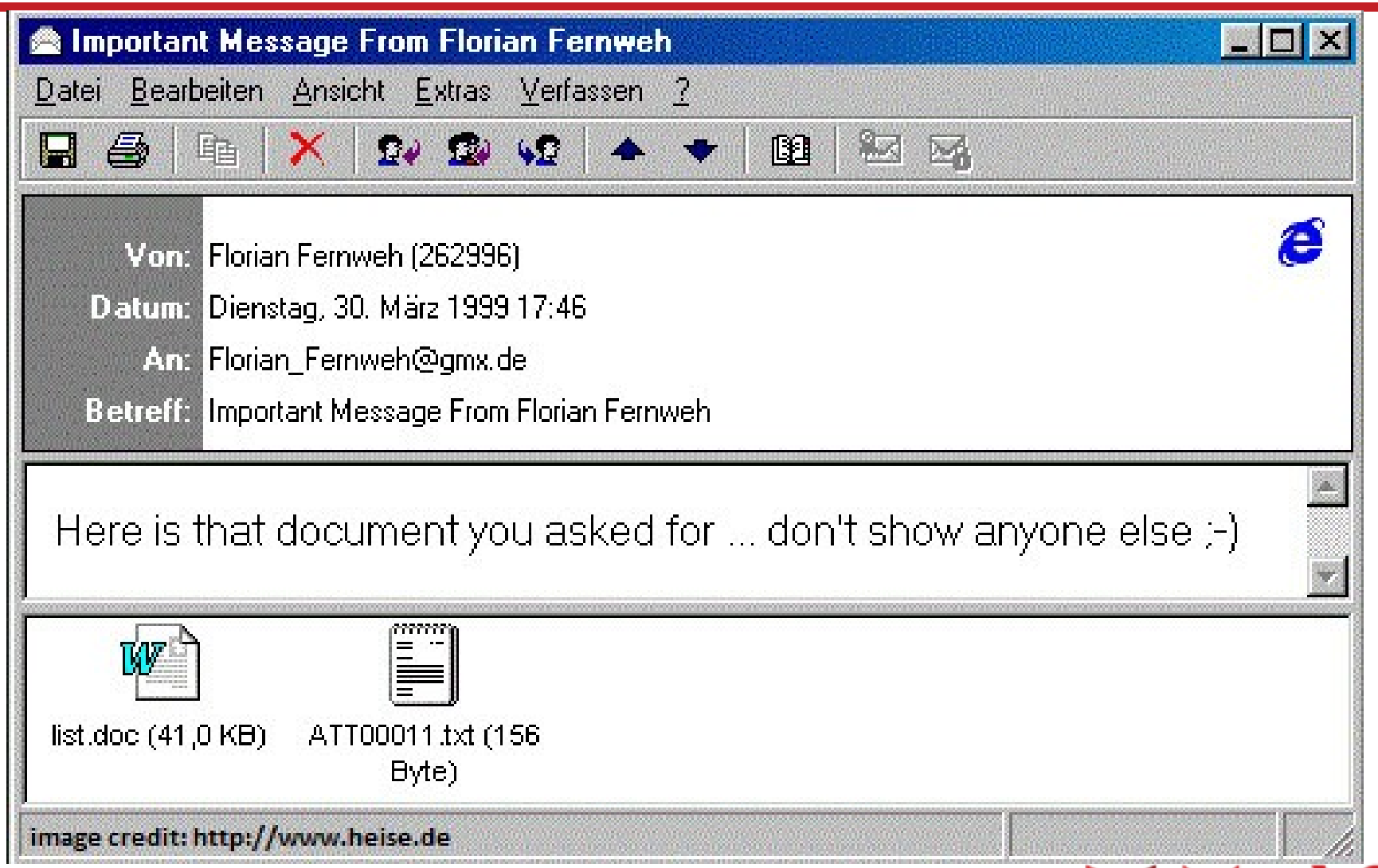


McAfee by Intel

1994-1998

- OneHalf
- Concept (Macro Word)
- Ply
- Laroux (Excel)
- Staog (Linux)
- CIH

1999 - Melissa



McAfee by Intel

1999 - Melissa

- Plataforma: W32
- Vector: e-mail (mass-mailing virus)
- Macro virus (escrito en VBS)
- Autor: David L. Smith
- Causó daños por U$D80 millones
- Sentenciado a 10 años de cárcel (cumplió sólo 20 meses por ~~soplón~~ “ayudar” al FBI)

McAfee by Intel

DEMO!! The good old days...

McAfee™
by Intel

2000 – I Love You

From: John Doe Sent: Thu 5/4/00 11:29 AM
To: John Doe
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER

LOVE-LETTER-FOR-YOU.TXT.vbs

coming from me.

McAfee by Intel

2000 – I Love You

- Plataforma: W32
- Vector: e-mail (mass-mailing virus)
- Worm (escrito en VBS)
- Autor: Onel de Guzmán
- Infectó más de 50 millones de computadoras
- Causó pérdidas por U$D 5500 millones
- 5 días después, había 18 mutaciones
- Fue detenido y liberado más tarde.

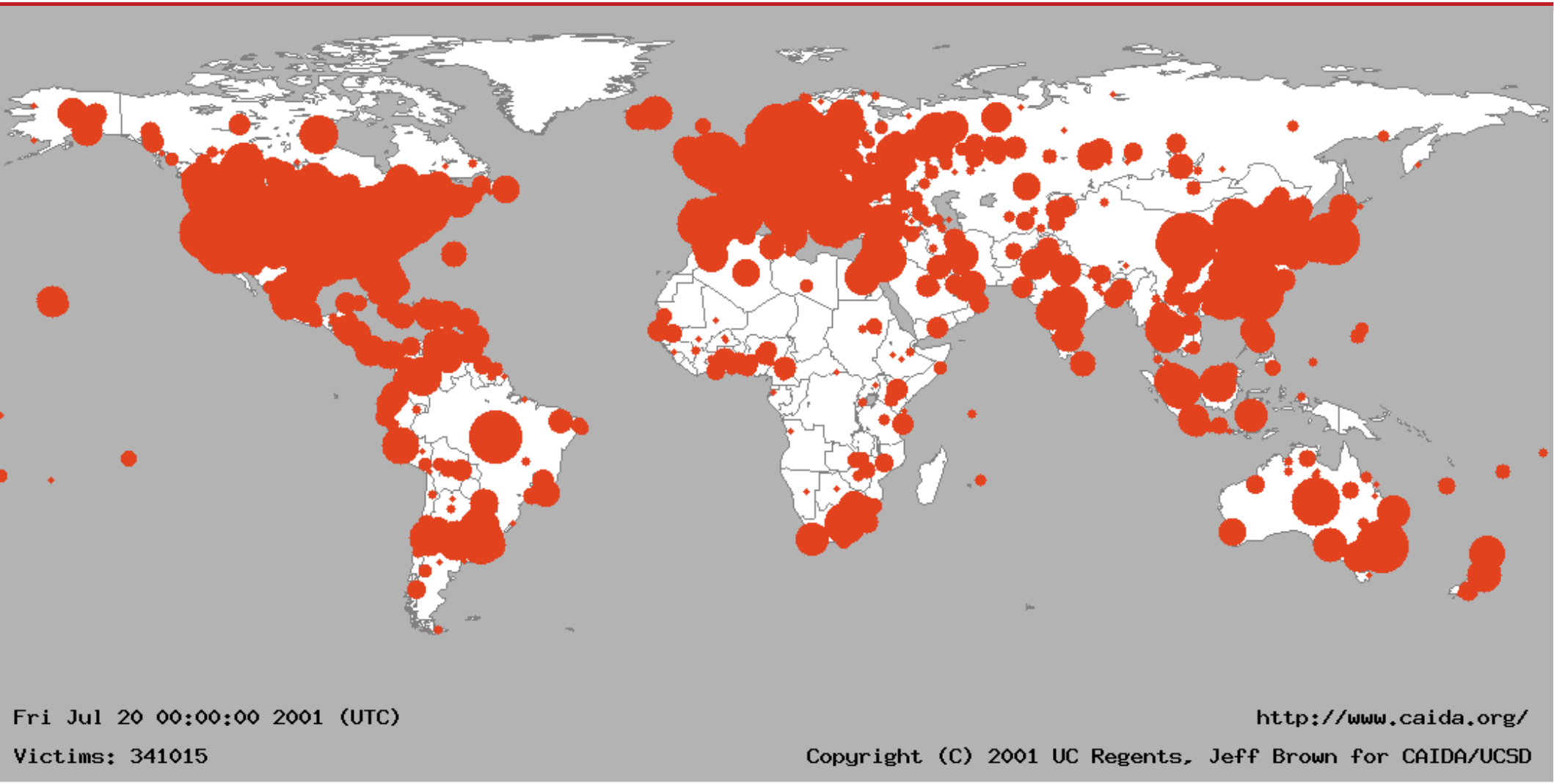
McAfee by Intel

2001 – Code Red

- Plataforma: W32
- Vector: Vulnerabilidad de IIS (Buffer overflow)
- Worm (Assembler)
- Autor: China? No se sabe realmente
- No se copia a sí mismo, sólo residente en memoria
- Causaba un DDoS a www.whitehouse.gov, cambiaba entradas de registro para obtener acceso remoto

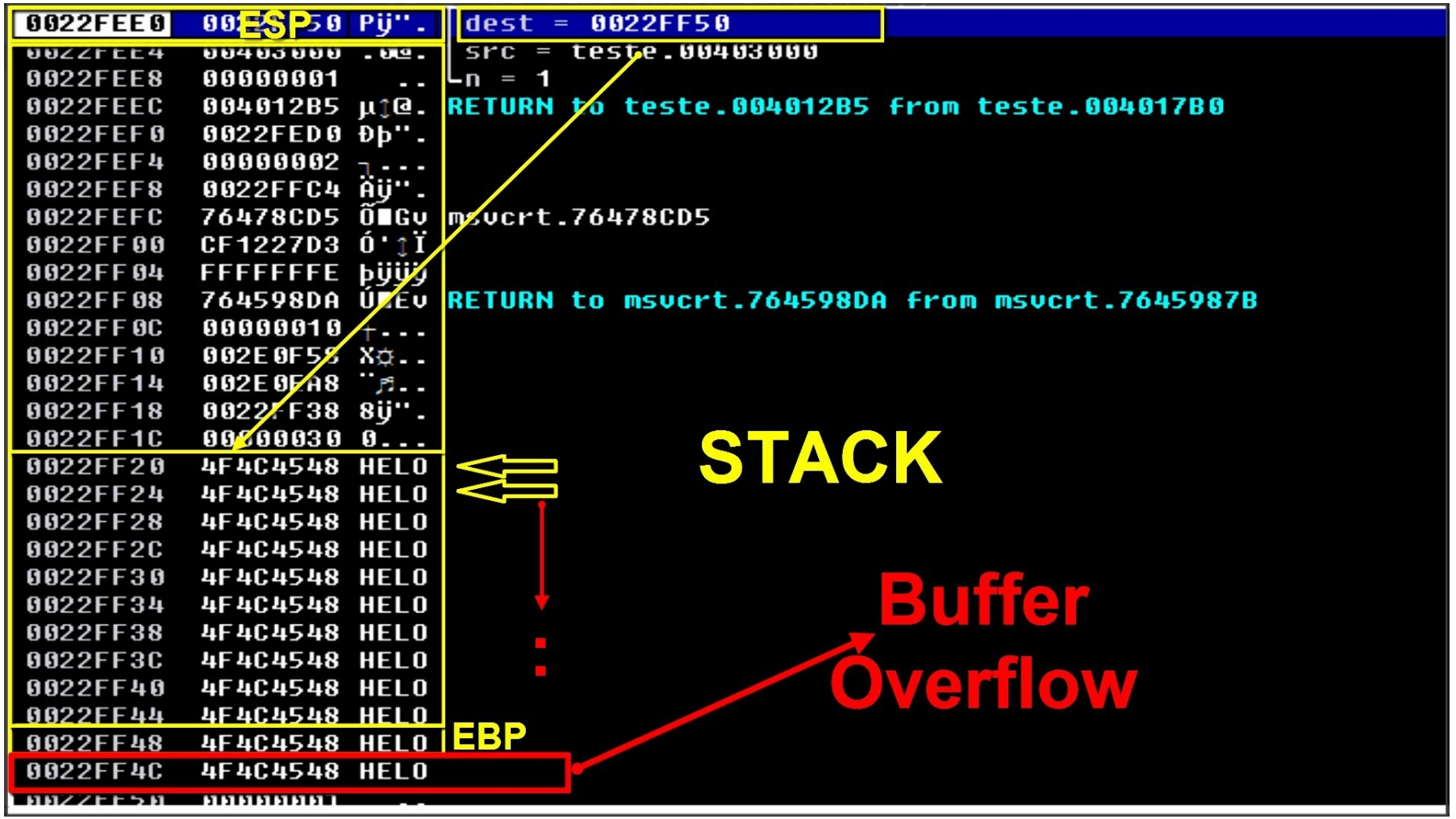
McAfee by Intel

2001 – Code Red



McAfee by Intel

¿Cómo funciona un Buffer Overflow?



McAfee by Intel

2001 – Anna Kurnikova

- Plataforma: W32
- Vector: e-mail (mass-mailing virus)
- Worm
- Autor: Jan De Vit
- Uso un generador creado por “[K]Alamar”
- No corrompía el sistema infectado
- Sentenciado a 150hs de servicio comunitario

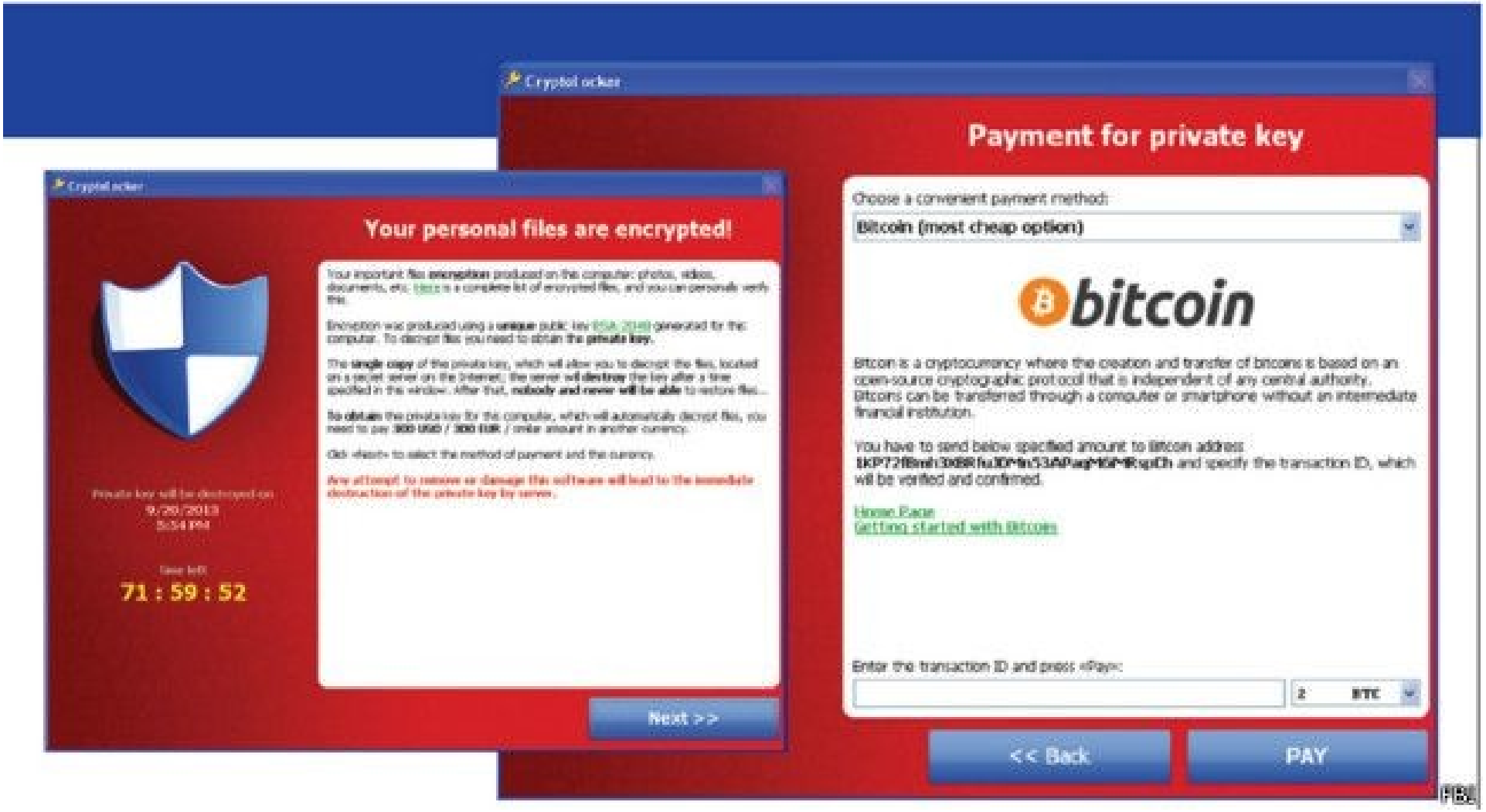
McAfee by Intel

+/-2013 Ransonware

- Programa que restringe el acceso a archivos (encriptación).
- Pide rescate ($ - BTC) por los datos.
- Según informe de McAfee, se está pagando al rededor de U$D 100.000

McAfee by Intel

+/-2013 CryptoLocker



McAfee by Intel

+/-2013 CryptoLocker

- Plataforma: W32
- Vector: e-mail o botnet Zeus
- Ransomware - Troyano
- Autor: Evgeniy Bogachev
- Encriptaba el sistema con RSA 2048 bits
- Se estima que robó al rededor de U$D 3 millones

McAfee by Intel

+/-2013 CryptoLocker

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

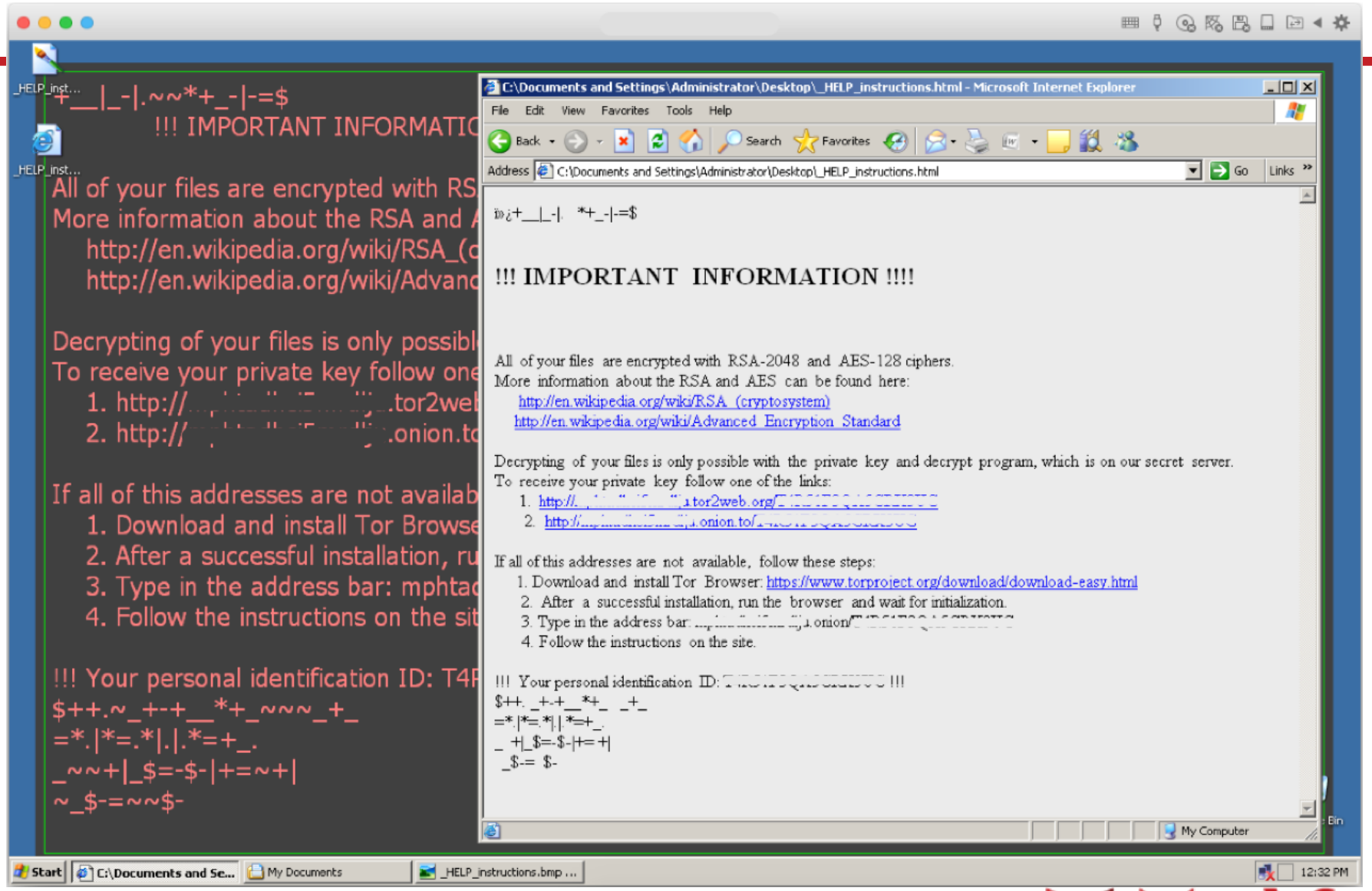
EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

FBI

McAfee by Intel

2016 - Locky



McAfee by Intel

2016 - Locky

- Plataforma: W32
- Vector: e-mail con macros de Word
- Ransomware - Troyano
- Autor: ?
- Algunas variantes detectan si se ejecuta en una VM y relocación del código
- También se distribuye en Js

McAfee by Intel

APTs

- Es más bien un proceso de hacking.
- Generalmente se usan distintos malwares para controlar y extraer datos.
- Grupos criminales organizados (compañías, estados)

Lifecycle

- Initial compromise – zero-day viruses / exploits
- Establish Foothold – remote administration software
- Escalate Privileges
- Internal Reconnaissance – collect information on surrounding infrastructure
- Move Laterally – expand control to other workstations
- Maintain Presence
- Complete Mission – extraer información

McAfee by Intel

Operación Aurora

McAfee™
by Intel

2009/10 Operación Aurora

- Llevado a cabo por Elderwood (China)
- Ataque coordinado a: Google, Adobe, Yahoo, Symantec, Morgan Stanley, entre otros.
- Robaron información e intentaron ingresar a correos de disidentes.
- Usaron vulnerabilidades “zero-day” de IE.

McAfee by Intel

Operación Aurora

McAfee™
by Intel

2010 - Stuxnet

2010 - Stuxnet

- Worm que atacaba computadoras industriales
- Target: Programa Nuclear de Irán
- Creado bajo la administración Bush en conjunto con Israel
- Atacaba computadoras Windows, sistemas SCADA y PLCs
- Arruinó 1/5 de los centrifugadores Iraníes

McAfee by Intel

Algunas consecuencias

- 1998 - Robert Morris (Morris worm) – Profesor del MIT.
- Chen Ing Hau (Chernobyl) – Fue apresado y liberado por no haber legislación.
- Sven Jaschan (Netsky – Sasser) – denunciado por un amigo, juzgado como menor, 21 meses en prisión.
- Chris Pile (Pathogen) – 18 meses en prisión.

Q&A

McAfee™
by Intel

Info

- https://www.av-test.org/en/statistics/malware/
- https://www.cnet.com/news/melissa-virus-turns-10/
- https://kb.iu.edu/d/aehs
- http://itlaw.wikia.com/wiki/Virus_obfuscation_techniques
- Defcon : The History and evolution of malware

McAfee by Intel