

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 McAfee 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

Inscríbete en: <https://techdaymcafeebyinteleventbrite.es> • Cupos limitados!

Participan

ASC
ASCENTIO
TECHNOLOGIES

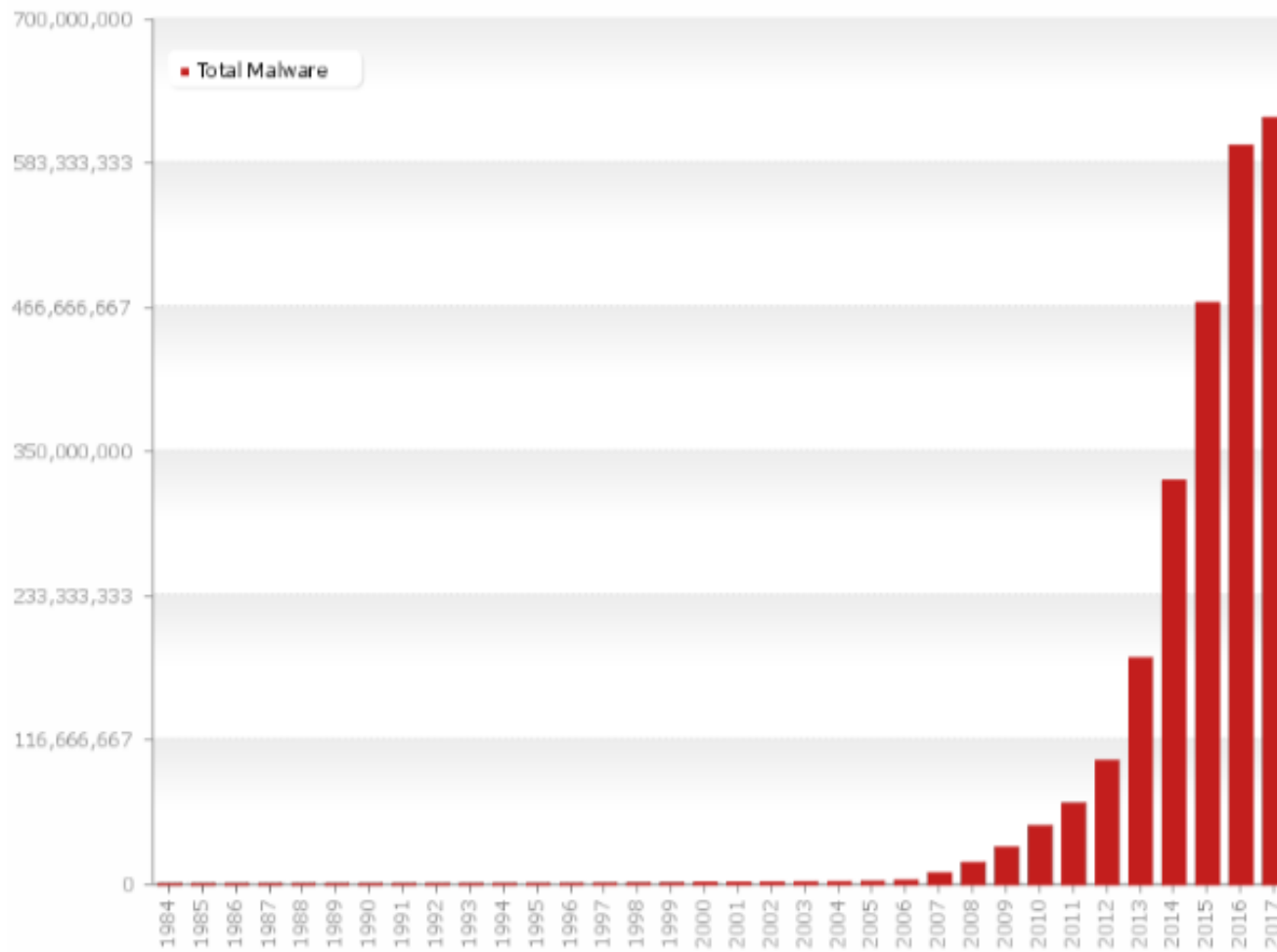


Olapic



Cuántos?

- Se registran 390.000 programas maliciosos por día.



Last update: 03-20-2017 10:38

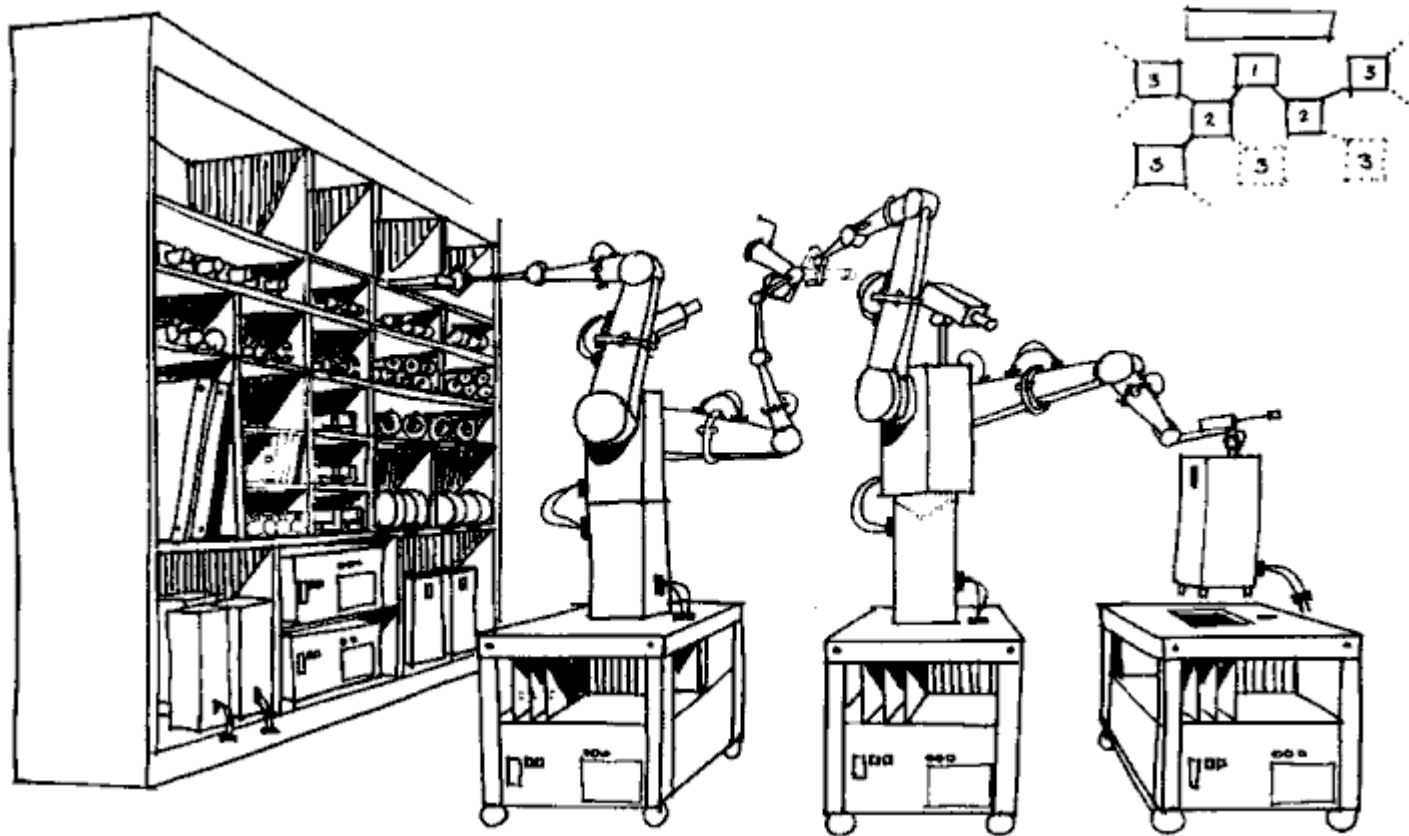
Copyright © AV-TEST GmbH, www.av-test.org

Dónde comenzó todo

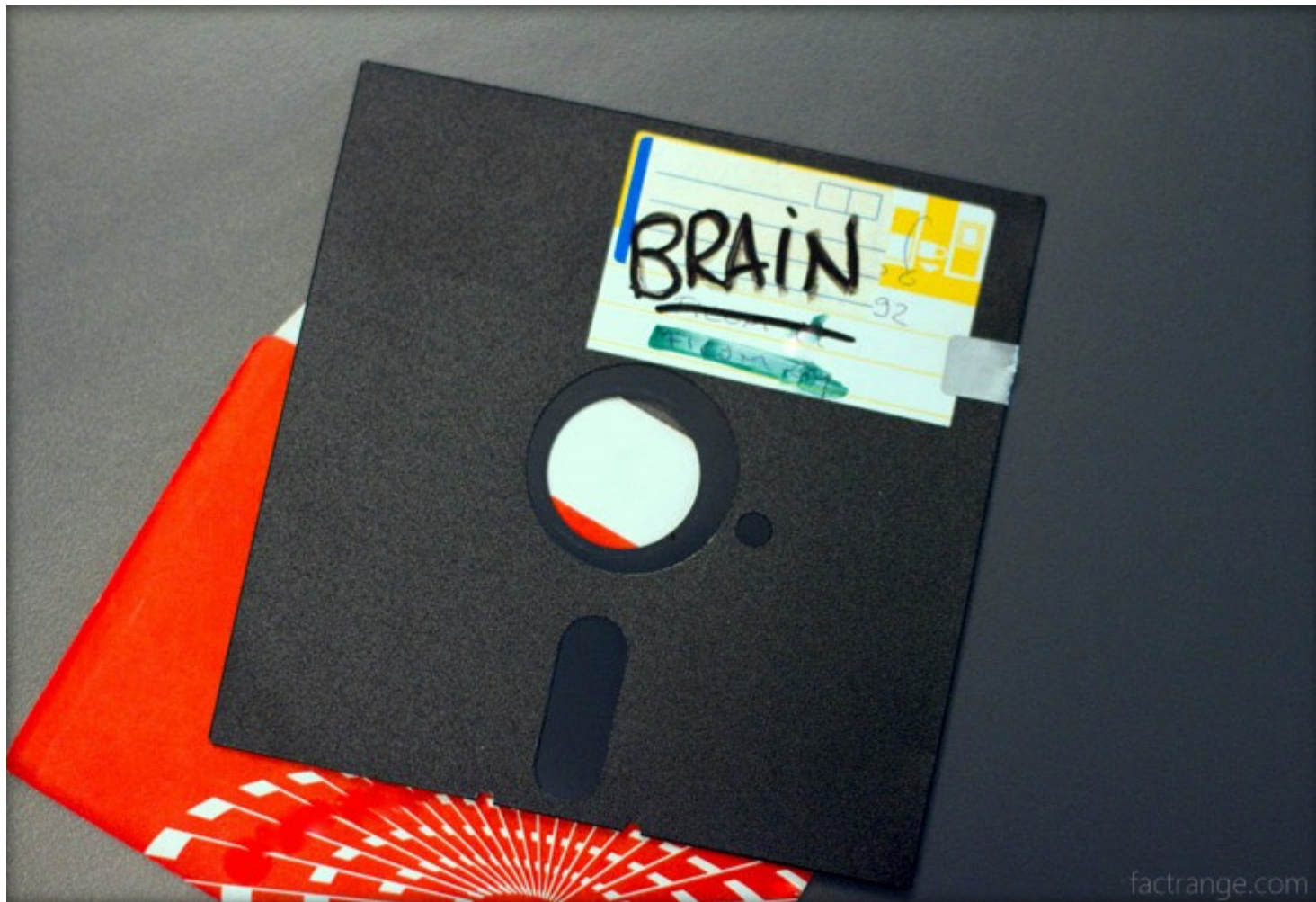
- 1949 - John von Neumann "Theory of self-reproducing automata"



Self-reproducing automata



1986



1986 - Brain

- Creado por Basit y Alvi Amjad (Pakistán)



1986 - Brain

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

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

The Little Black Book of Computer Viruses

Electronic Edition

By
Mark
Ludwig

- Se puede bajar de internet!

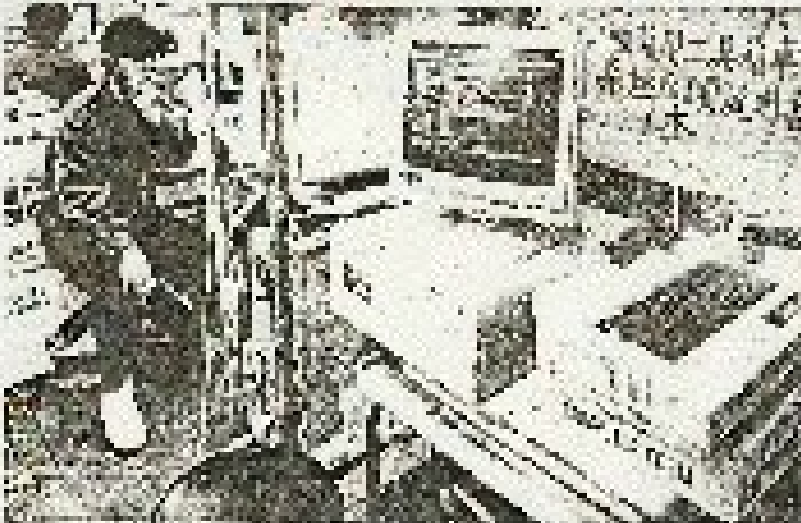
1991 - Michelangelo

1997-1998

DATE: 11/11/2011 11:11:11 AM

YOUR LEISURE READING

Michelangelo virus attacks P.C. data worldwide



Dr. Shing-Ping Wan, Institute of Mathematics, The Chinese University of Hong Kong, Shatin, New Territories, Hong Kong, completed his undergraduate education at the Chinese University of Hong Kong, and received his MSc and PhD degrees from the Chinese University of Hong Kong. He is currently an associate professor at the Chinese University of Hong Kong. His research interests include algebraic combinatorics, algebraic geometry, and algebraic topology.

WILLIAM WILSON has been
teaching English and all other
languages in various schools in
the United States for many
years. He is now in charge
of the English department at
the University of California,
Berkeley.

The authors thank Joseph and
Susan D. L. for their generous
support of this research. We also
thank the following for their
contributions to this research: the
staff of the University of
California, San Diego, and the
University of California, Los Angeles.

What makes *McVie* so enjoyable is that it's a pop record. The music is a little more sophisticated than the previous albums, but it's still a pop record. It's a record that's easy to listen to, and it's a record that's easy to love. It's a record that's a little different from the others, but it's a record that's still a pop record. It's a record that's a little different from the others, but it's a record that's still a pop record. It's a record that's a little different from the others, but it's a record that's still a pop record.

[illegible]

1. *What is the main reason for the decline in the number of people who are members of the Church of England?*
 2. *What are the main reasons for the decline in the number of people who are members of the Church of England?*
 3. *What are the main reasons for the decline in the number of people who are members of the Church of England?*

The *Journal of the American Veterinary Medical Association* is the largest and most influential of the specialty journals. It is published by the American Veterinary Medical Association, which is the largest and most influential of the specialty associations. The *Journal* is published by the American Veterinary Medical Association, which is the largest and most influential of the specialty associations.

— **1998** —

has a 100% match of genes and has
 100% match with matching proteins
 name of

by Peter

For more information, contact
Lynne H. Mendenhall, Director,
New York Small Business
Fund and Small Business
Fund, Inc., at (212) 312-2000.
MAILING LIST: For more infor-
mation, contact the Small Business
Fund, Inc., 200 West 42nd Street,
New York, NY 10018-3000.

the long-term effects of these
energy saving measures and how
they will affect the economy, with
particular emphasis on the energy
sector.

After the 1990 election, and until 1995, many political groups were said to be "bigger" because of the increase in the number of elected officials. During this period, the U.S. Supreme Court ruled that 11 groups were "too big" to be considered "persons" for purposes of the 14th Amendment.

These people are called "movers" and are responsible for the work of moving the books from the old location to the new one. They are also responsible for the work of moving the books from the old location to the new one.

In February, involving 20 management staff, a total of 100,000 yen for a group of 10 persons of the company was requested. During the visit, the staff of the company were asked to provide information on the company's business and the company's financial situation.

[illegible]

During the 1980s, the number of deaths attributed to the epidemic of AIDS has grown, with the number of deaths in 1989 estimated at more than 1 million. Public health officials are

Marlow and his crew, including his wife, also discovered the dead man, and a few minutes later, one of the boatmen saw another victim, making a total of three dead men and one woman. The boatmen were shocked and did not know how to react.

Widened

© 2005 Blackwell Publishing Ltd, *Journal of Internal Medicine* 258: 103–110

1. *gemmae*.
 2. *gemmae*.
 3. *gemmae*.
 4. *gemmae*.
 5. *gemmae*.
 6. *gemmae*.
 7. *gemmae*.
 8. *gemmae*.
 9. *gemmae*.
 10. *gemmae*.
 11. *gemmae*.
 12. *gemmae*.
 13. *gemmae*.
 14. *gemmae*.
 15. *gemmae*.
 16. *gemmae*.
 17. *gemmae*.
 18. *gemmae*.
 19. *gemmae*.
 20. *gemmae*.
 21. *gemmae*.
 22. *gemmae*.
 23. *gemmae*.
 24. *gemmae*.
 25. *gemmae*.
 26. *gemmae*.
 27. *gemmae*.
 28. *gemmae*.
 29. *gemmae*.
 30. *gemmae*.
 31. *gemmae*.
 32. *gemmae*.
 33. *gemmae*.
 34. *gemmae*.
 35. *gemmae*.
 36. *gemmae*.
 37. *gemmae*.
 38. *gemmae*.
 39. *gemmae*.
 40. *gemmae*.
 41. *gemmae*.
 42. *gemmae*.
 43. *gemmae*.
 44. *gemmae*.
 45. *gemmae*.
 46. *gemmae*.
 47. *gemmae*.
 48. *gemmae*.
 49. *gemmae*.
 50. *gemmae*.
 51. *gemmae*.
 52. *gemmae*.
 53. *gemmae*.
 54. *gemmae*.
 55. *gemmae*.
 56. *gemmae*.
 57. *gemmae*.
 58. *gemmae*.
 59. *gemmae*.
 60. *gemmae*.
 61. *gemmae*.
 62. *gemmae*.
 63. *gemmae*.
 64. *gemmae*.
 65. *gemmae*.
 66. *gemmae*.
 67. *gemmae*.
 68. *gemmae*.
 69. *gemmae*.
 70. *gemmae*.
 71. *gemmae*.
 72. *gemmae*.
 73. *gemmae*.
 74. *gemmae*.
 75. *gemmae*.
 76. *gemmae*.
 77. *gemmae*.
 78. *gemmae*.
 79. *gemmae*.
 80. *gemmae*.
 81. *gemmae*.
 82. *gemmae*.
 83. *gemmae*.
 84. *gemmae*.
 85. *gemmae*.
 86. *gemmae*.
 87. *gemmae*.
 88. *gemmae*.
 89. *gemmae*.
 90. *gemmae*.
 91. *gemmae*.
 92. *gemmae*.
 93. *gemmae*.
 94. *gemmae*.
 95. *gemmae*.
 96. *gemmae*.
 97. *gemmae*.
 98. *gemmae*.
 99. *gemmae*.
 100. *gemmae*.
 101. *gemmae*.
 102. *gemmae*.
 103. *gemmae*.
 104. *gemmae*.
 105. *gemmae*.
 106. *gemmae*.
 107. *gemmae*.
 108. *gemmae*.
 109. *gemmae*.
 110. *gemmae*.
 111. *gemmae*.
 112. *gemmae*.
 113. *gemmae*.
 114. *gemmae*.
 115. *gemmae*.
 116. *gemmae*.
 117. *gemmae*.
 118. *gemmae*.
 119. *gemmae*.
 120. *gemmae*.
 121. *gemmae*.
 122. *gemmae*.
 123. *gemmae*.
 124. *gemmae*.
 125. *gemmae*.
 126. *gemmae*.
 127. *gemmae*.
 128. *gemmae*.
 129. *gemmae*.
 130. *gemmae*.
 131. *gemmae*.
 132. *gemmae*.
 133. *gemmae*.
 134. *gemmae*.
 135. *gemmae*.
 136. *gemmae*.
 137. *gemmae*.
 138. *gemmae*.
 139. *gemmae*.
 140. *gemmae*.
 141. *gemmae*.
 142. *gemmae*.
 143. *gemmae*.
 144. *gemmae*.
 145. *gemmae*.
 146. *gemmae*.
 147. *gemmae*.
 148. *gemmae*.
 149. *gemmae*.
 150. *gemmae*.
 151. *gemmae*.
 152. *gemmae*.
 153. *gemmae*.
 154. *gemmae*.
 155. *gemmae*.
 156. *gemmae*.
 157. *gemmae*.
 158. *gemmae*.
 159. *gemmae*.
 160. *gemmae*.
 161. *gemmae*.
 162. *gemmae*.
 163. *gemmae*.
 164. *gemmae*.
 165. *gemmae*.
 166. *gemmae*.
 167. *gemmae*.
 168. *gemmae*.
 169. *gemmae*.
 170. *gemmae*.
 171. *gemmae*.
 172. *gemmae*.
 173. *gemmae*.
 174. *gemmae*.
 175. *gemmae*.
 176. *gemmae*.
 177. *gemmae*.
 178. *gemmae*.
 179. *gemmae*.
 180. *gemmae*.
 181. *gemmae*.
 182. *gemmae*.
 183. *gemmae*.
 184. *gemmae*.
 185. *gemmae*.
 186. *gemmae*.
 187. *gemmae*.
 188. *gemmae*.
 189. *gemmae*.
 190. *gemmae*.
 191. *gemmae*.
 192. *gemmae*.
 193. *gemmae*.
 194. *gemmae*.
 195. *gemmae*.
 196. *gemmae*.
 197. *gemmae*.
 198. *gemmae*.
 199. *gemmae*.
 200. *gemmae*.
 201. *gemmae*.
 202. *gemmae*.
 203. *gemmae*.
 204. *gemmae*.
 205. *gemmae*.
 206. *gemmae*.
 207. *gemmae*.
 208. *gemmae*.
 209. *gemmae*.
 210. *gemmae*.
 211. *gemmae*.
 212. *gemmae*.
 213. *gemmae*.
 214. *gemmae*.
 215. *gemmae*.
 216. *gemmae*.
 217. *gemmae*.
 218. *gemmae*.
 219. *gemmae*.
 220. *gemmae*.
 221. *gemmae*.

[illegible]

but remains due the
and needs an independent
from 1988.

After 1968, when the work of the *Journal* had an effect on the American movement, the *Journal* was no longer a journal of the movement. It was a journal of the movement.

only Baltimore, a spokesman said, and that of the other two had not yet been received. When Washington, D.C., has the publicity, it is probably not far off for some time. "It's the power of the press," he said.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1

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 días 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

Vector de transmisión

Universidad Tecnológica Nacional
Facultad Regional Cordoba

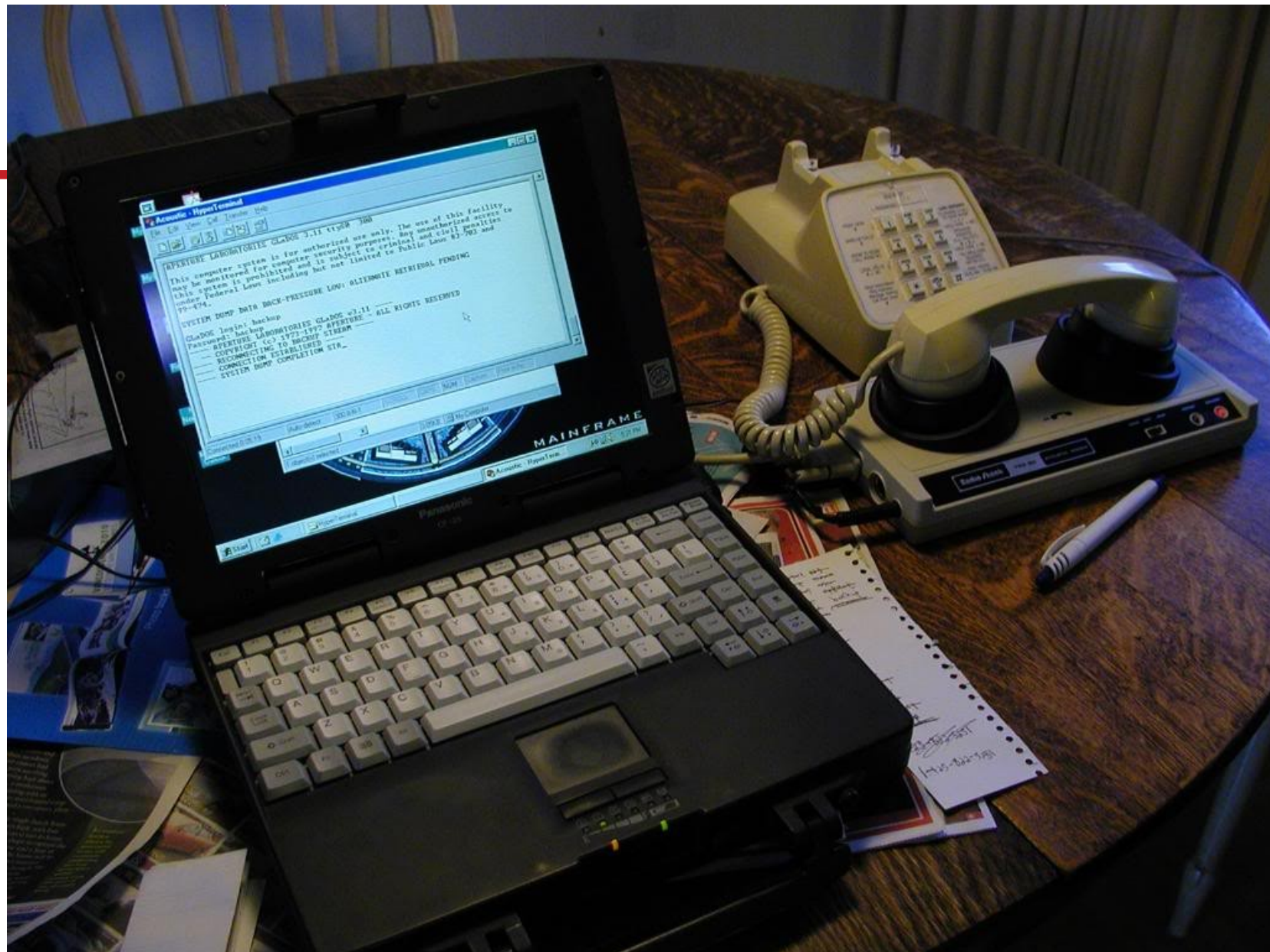
Bienvenido a la UTNFERC BBS!

Ingrese su nombre de usuario o regístrese si es su primera entrada.

Login:

Password:

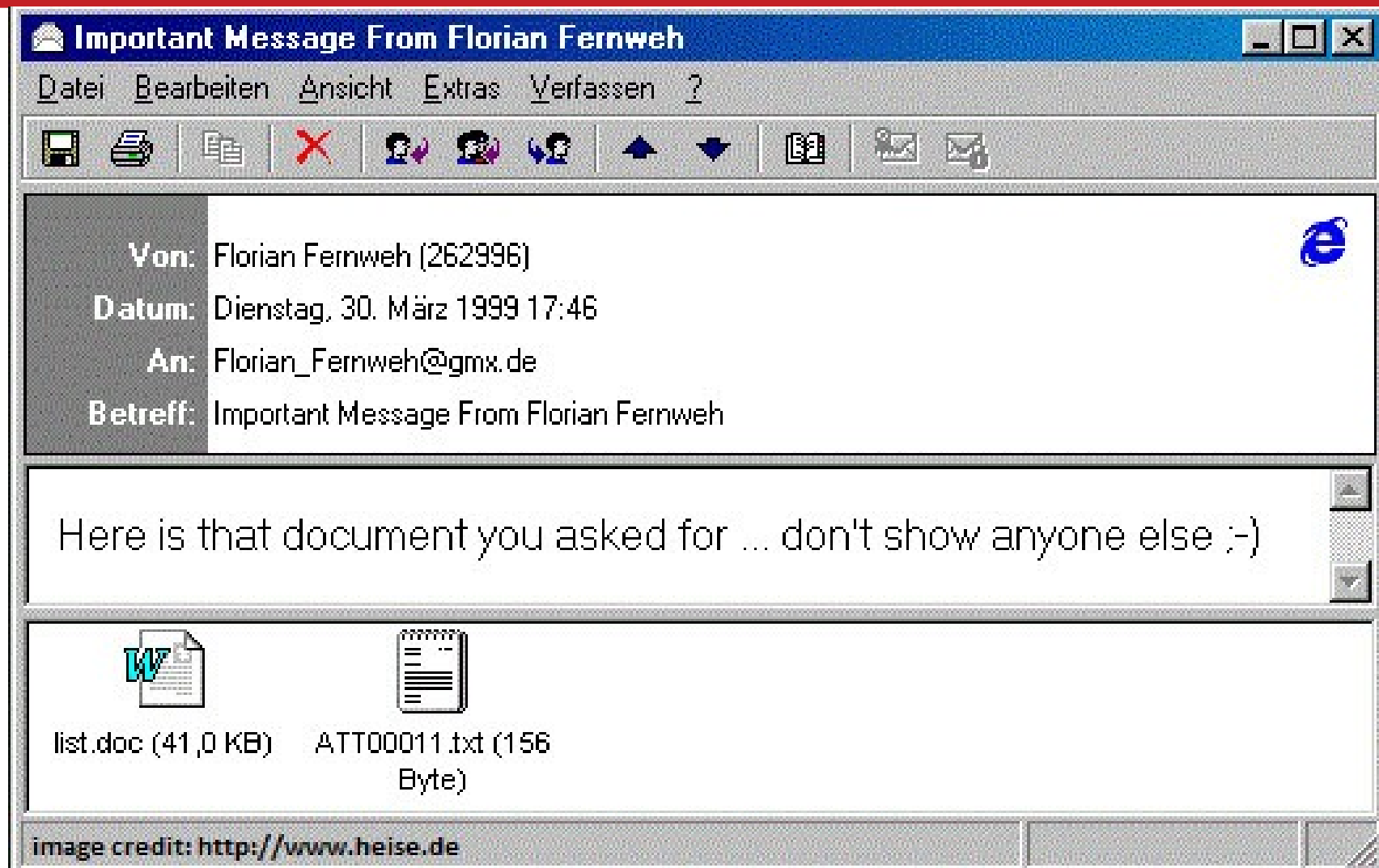
[Registración de nuevos usuarios](#)



1994-1998

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

1999 - Melissa



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 seplón “ayudar” al FBI)



DEMO!! The good old days...



2000 – I Love You



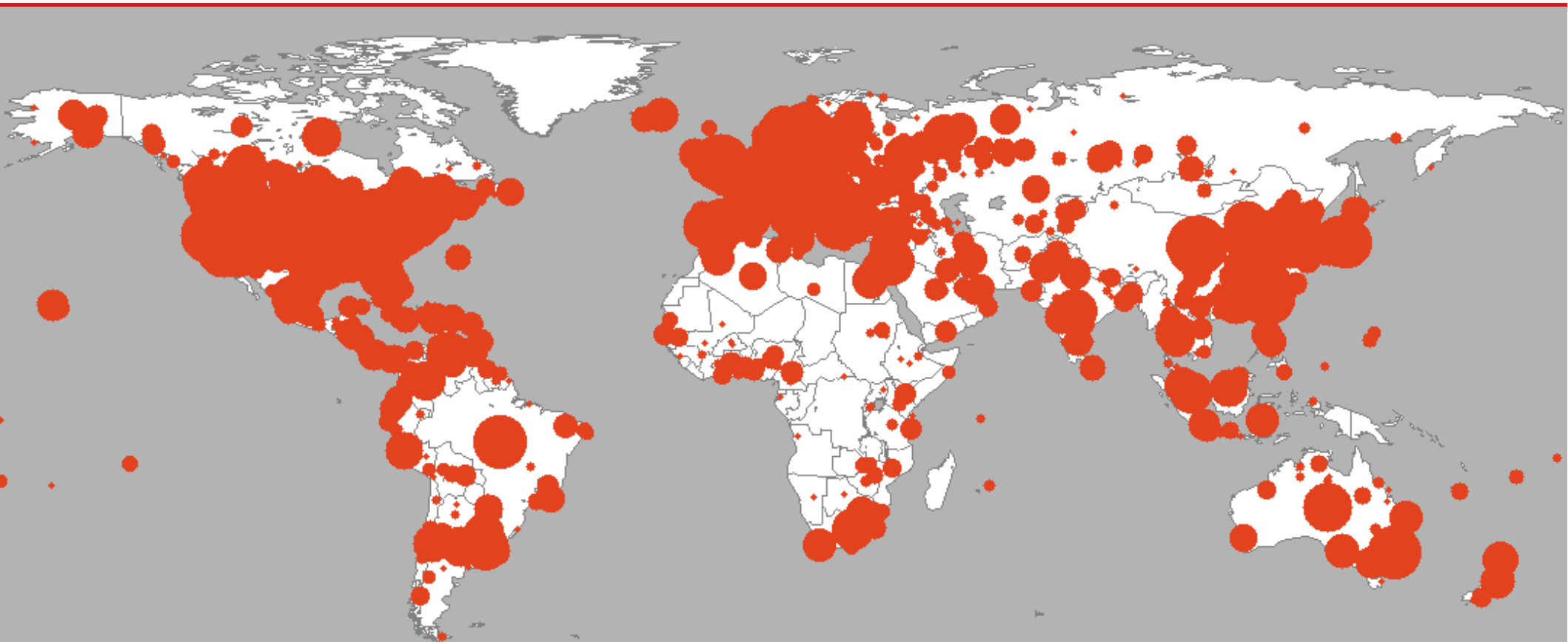
2000 – I Love You

- 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.

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

2001 – Code Red



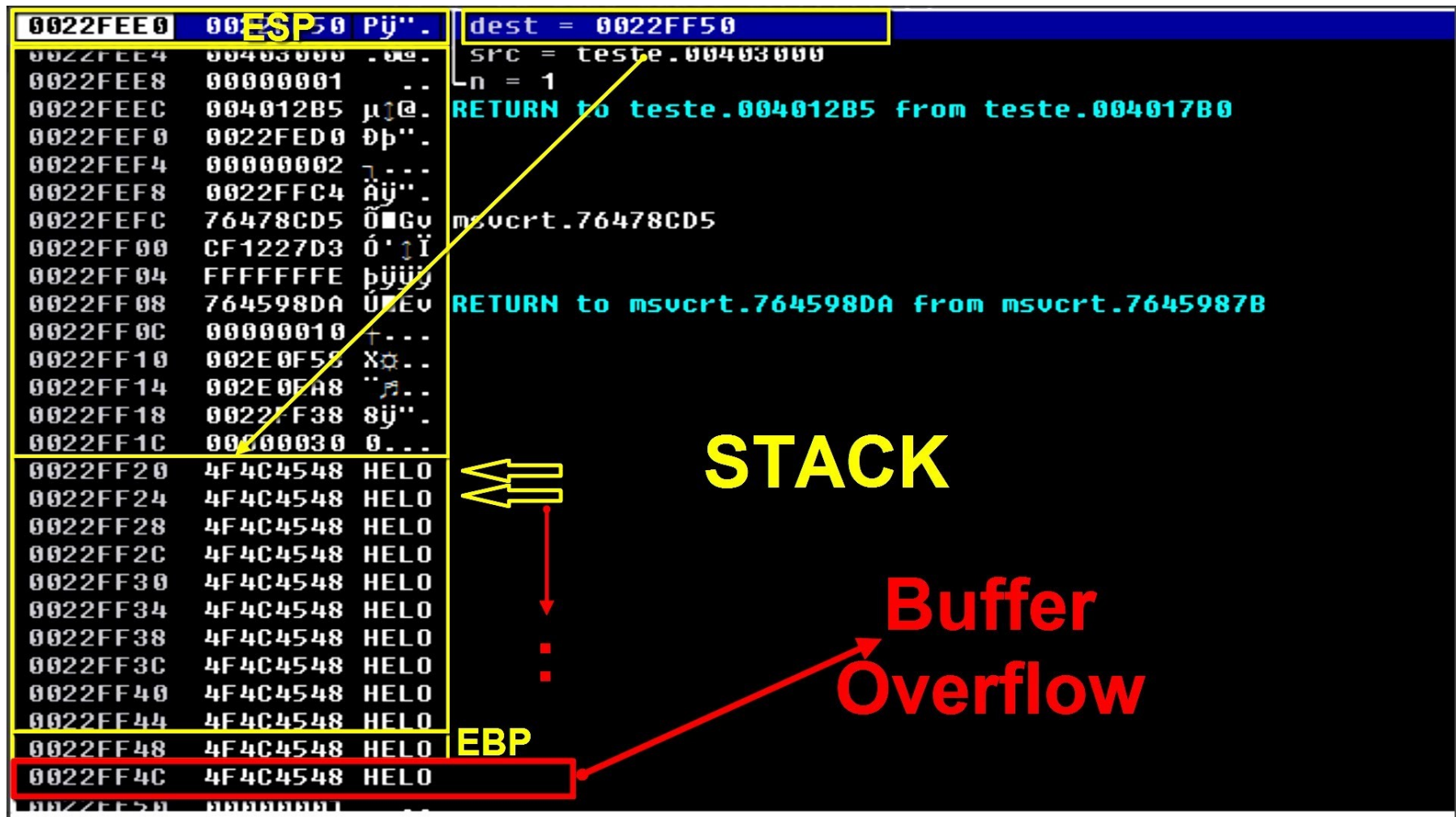
Fri Jul 20 00:00:00 2001 (UTC)

Victims: 341015

<http://www.caida.org/>

Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

¿Cómo funciona un Buffer Overflow?



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



+/-2013 Ransomware

- 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

+/-2013 CryptoLocker



+/-2013 CryptoLocker

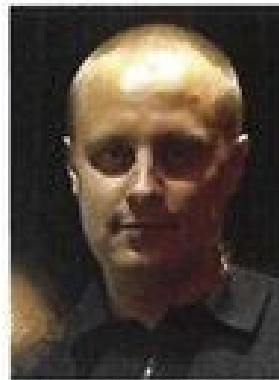
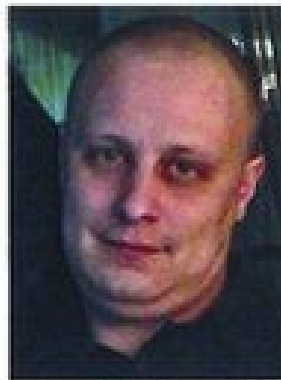
- Plataforma: W32
- Vector: e-mail o botnet Zeus
- Ransomware - Troyano
- Autor: Evgeniy Bogachev
- Encriptaba el sistema con RSA 2048 bits
- Se estima que robó al rededor de U\$D 3 millones

+/-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

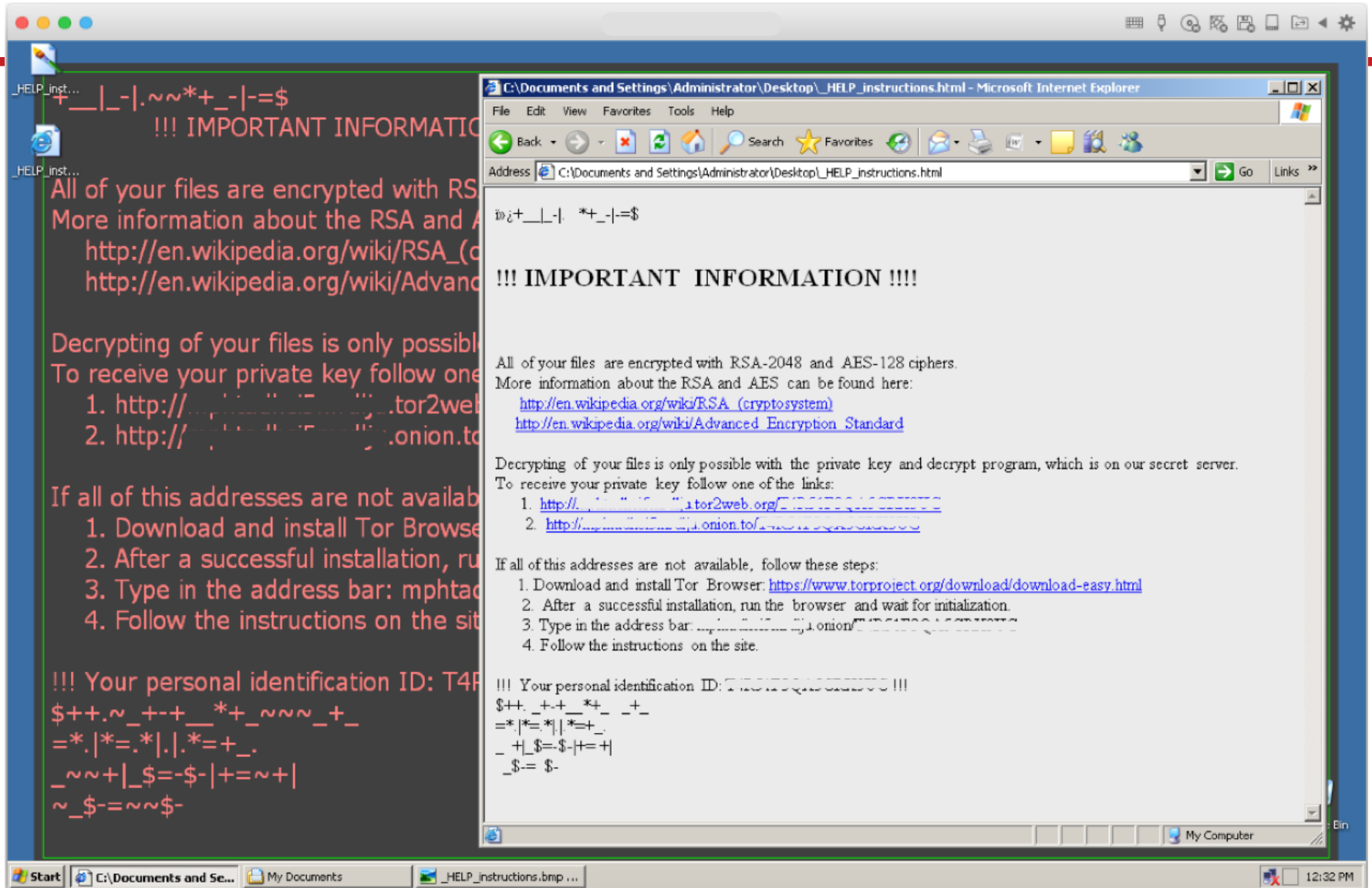


Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

FBI

 **McAfee**
by Intel

2016 - Locky



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

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

Operación Aurora



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.

Operación Aurora



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

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

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