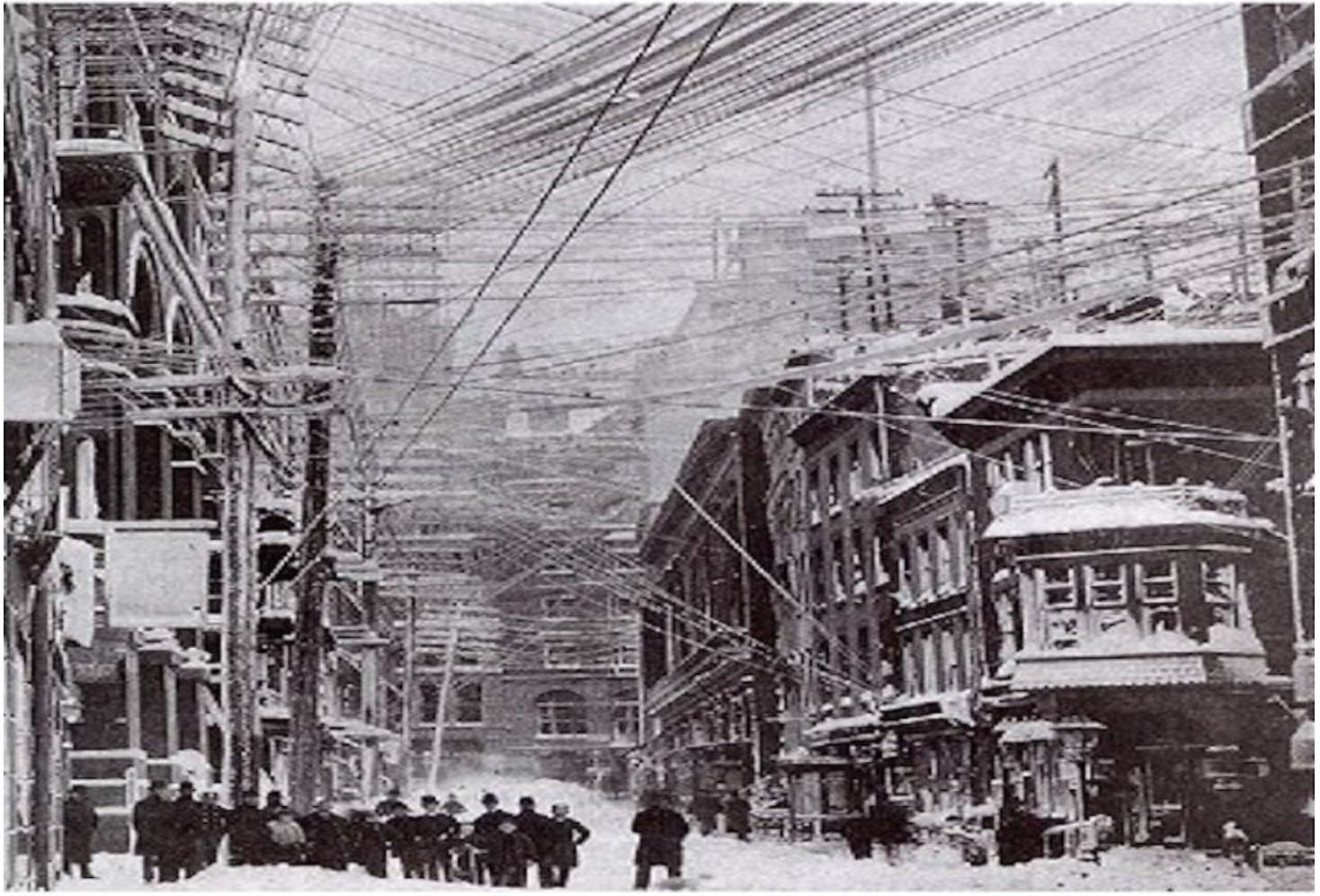
Historie počítačového viru

Předchůdci počítačového viru
Náhoda, šum a parazit v síti



- 40. léta - Nový komunikační model Shannona a Weavera, oddělení šumu od signálu
- Šum jako integrální součást moderní komunikace
- Virus lze popsat jako šum v komunikačním kanálu

Náhoda, šum a parazit v technologických sítích

- rušení signálu v telegrafických sítích

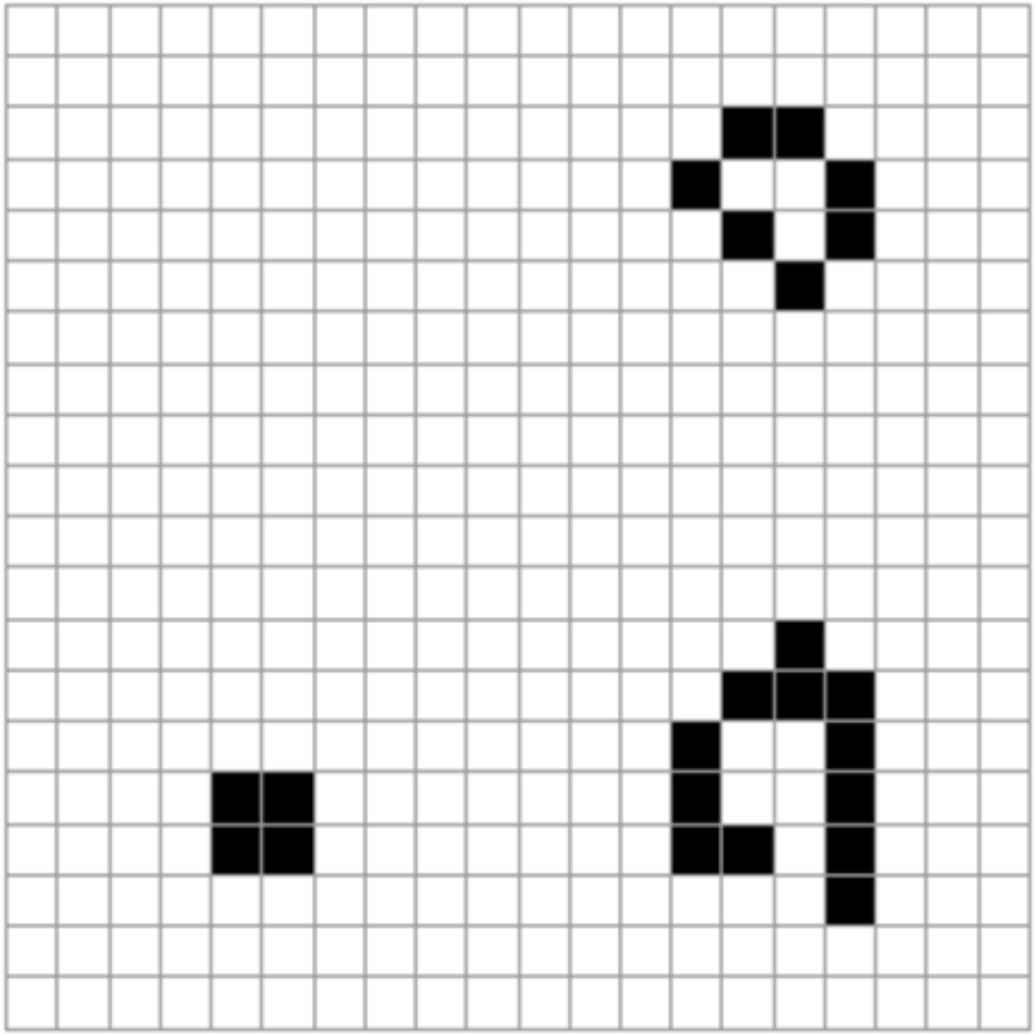
- Parazit v technologických sítích v 19.st. - člověk

1912 – Anarchie vln

Radioamatéři jako předchůdci hackerů

Předpoklady pro vznik počítačového viru (40. – 50. Léta)

- John von Neumann - Idea replikace – 40.léta
- myšlenka celulárního automatu, který reprodukuje sám sebe – kniha - Theory of Self-Reproducing Automata (1966)



- V 70. letech John Horton Conway zjednodušuje Neumannovy myšlenky a navrhuje systém s velmi jednoduchými pravidly vývoje

1. Živá buňka s méně než dvěma živými sousedy umírá (Příliš malá hustota populace)
2. Živá buňka s 2-3 živými sousedy přežívá do další generace
3. Živá buňka s více než třemi živými sousedy umírá (příliš velká hustota populace)
4. Mrtvá buňka s přesně třemi sousedy ožívá (reprodukce)

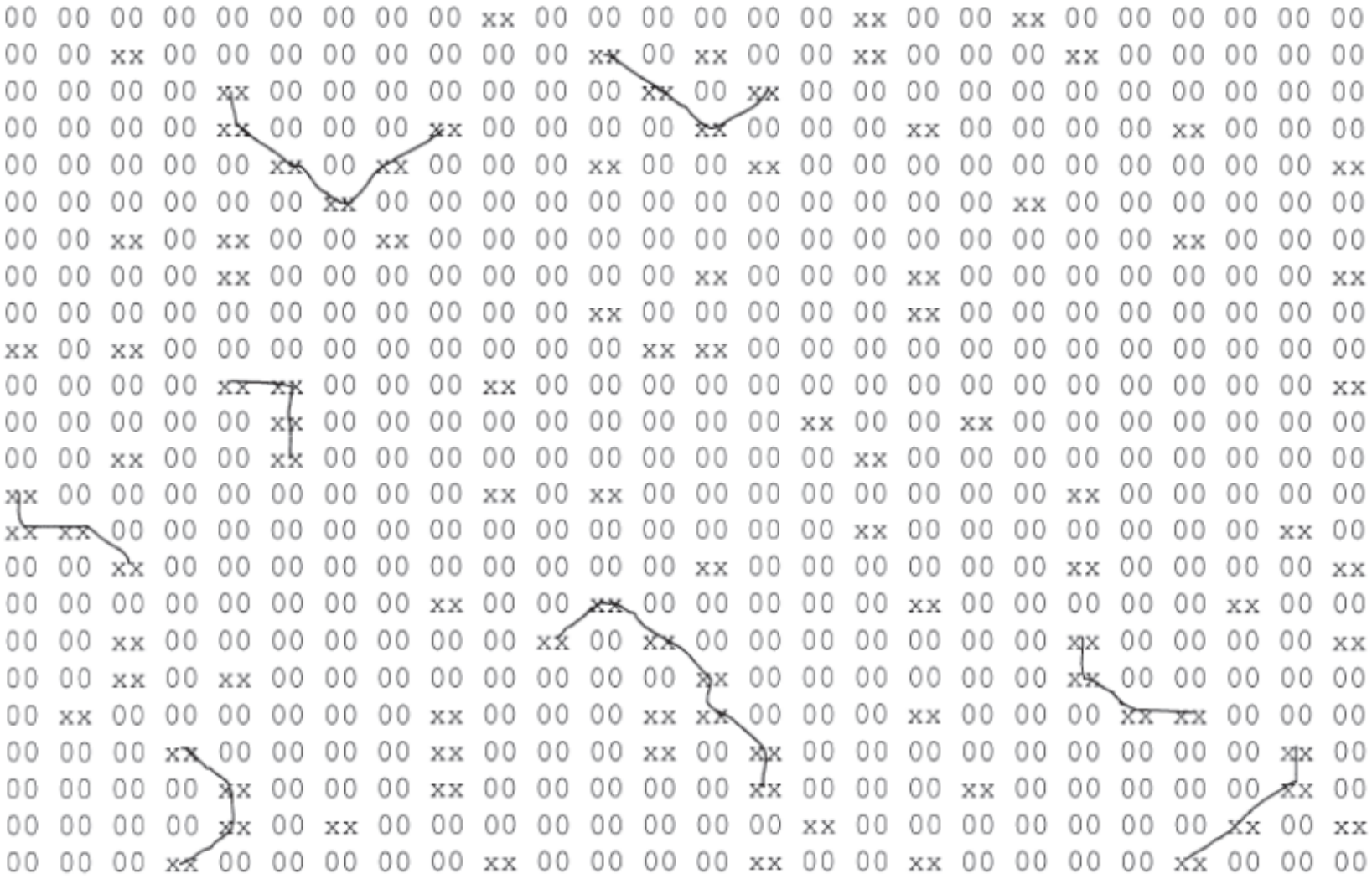
Game of life na Atari 2600 - https://www.youtube.com/watch?v=bSWhDHybXDY

Von Neumannova architektura

- 1. operační paměť
- 2. aritmeticko-logická jednotka
- 3. řadič – řídicí jednotka
- 4. vstupní zařízení
- 5. výstupní zařízení
- Univerzální struktura počítače
- Sekvenční zpracování dat
- Programy i data se uchovávají v téže operační paměti

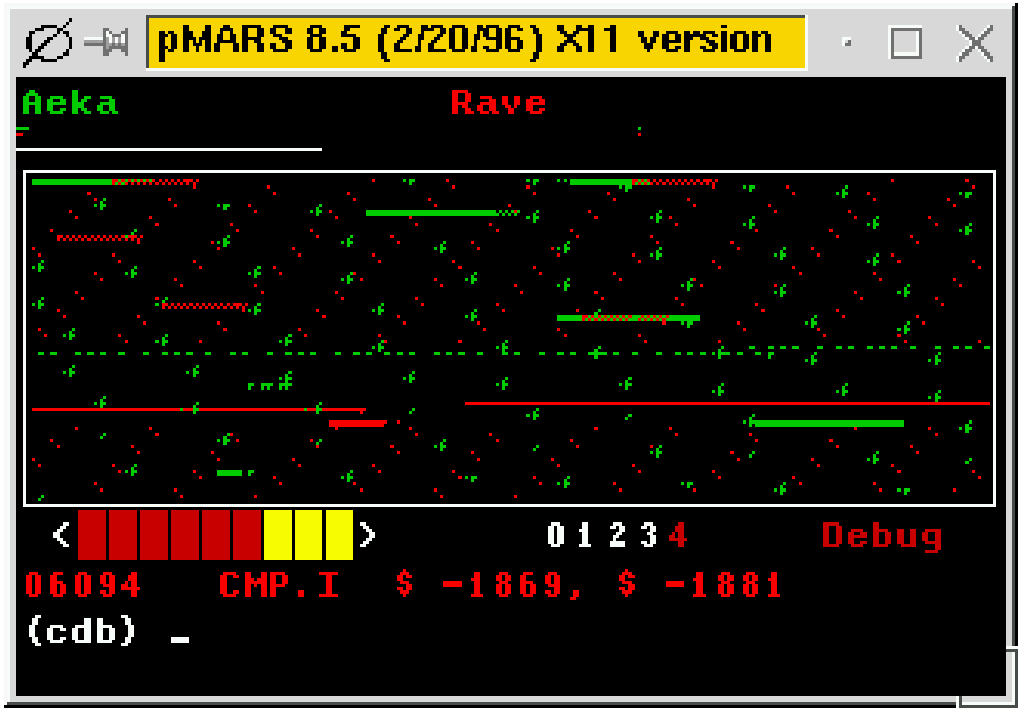
- programy podobné virům byly označovány jako červy – programy, jež narušovaly osobní prostor jiných programů, často produkovaly náhodné operace a chyby - důsledek této architektury
- kdybychom se pokusili sledovat stopu chybných operací odhalili bychom náhodné vzory paměťových lokací, v podobě nepravidelných zakřivených drah

Wormhole damage pattern



Užitečné, neškodné a zábavné samoreprodukční programy (60. -70. léta)

- Core wars (od 1961) – vzájemný boj programů
- https://www.youtube.com/watch?v=R2Qjc-dAD_k



- Cookie program (70. léta)
- Creeper (1971)
- ANIMAL (1975)
- XEROX worm (1979)

První nebezpečné viry, příchod osobních počítačů a nových hackerů, konstrukce virů ve vědeckém prostředí (80.léta)

- **Apple viry**
- Apple II (1977) první osobní počítač, který se rozšířil, ukázal, že počítač může být pro každého
- Platforma, na níž se objevily první viry psané přímo uživateli (většinou studenty)
- První pojmenovaný virus – Elk Cloner – 1981

Elk Cloner:
The program with a personality

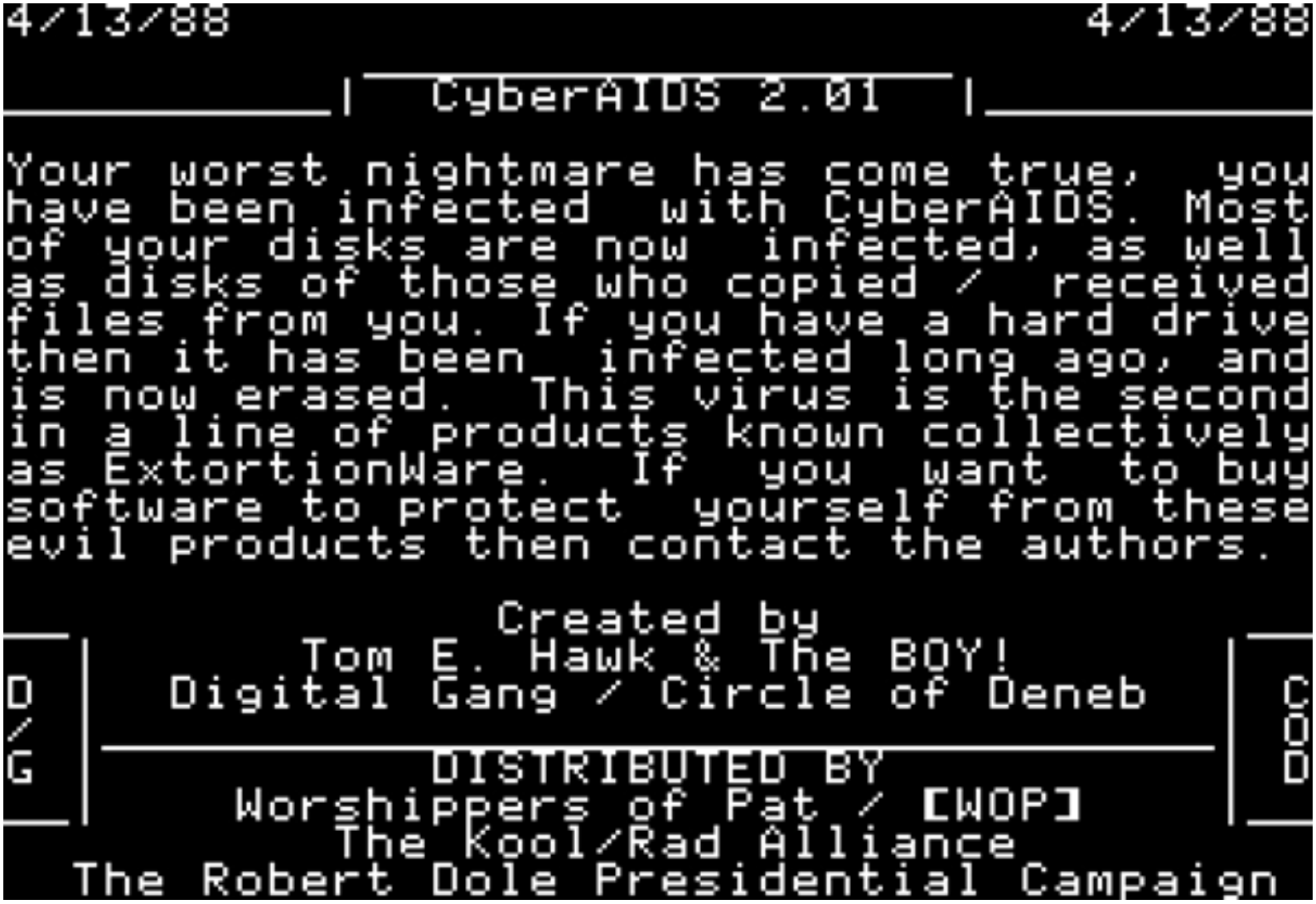
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

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

- Virus, který vytvořil Joe Dellinger v roce 1981
- chtěl vědět jak moc je nutné změnit kód operačního systému DOS 3.3, aby mohl kopírovat sám sebe jako virus
- Druhá verze viru způsobovala neočekávané poruchy
- Šířil se prostřednictvím pirátských kopií počítačové hry Congo Bongo

CyberAIDS – 1988 –

- vytvořen skupinou hackerů
- vydání Pro Dosu (1983), zaktivizovalo hackery chtěli vytvořit kopii systému, v níž bude obsažen virus
- Časté ztotožňování počítačového viru s virem HIV


4/13/88
4/13/88
CyberAIDS 2.01
Your worst nightmare has come true, you have been infected with CyberAIDS. Most of your disks are now infected, as well as disks of those who copied / received files from you. If you have a hard drive then it has been infected long ago, and is now erased. This virus is the second in a line of products known collectively as ExtortionWare. If you want to buy software to protect yourself from these evil products then contact the authors.
Created by
Tom E. Hawk & The BOY!
Digital Gang / Circle of Deneb
DISTRIBUTED BY
Worshippers of Pat / [WOP]
The Kool/Rad Alliance
The Robert Dole Presidential Campaign
D/G
COD

- Virus Festering Hate – od stejných autorů
- po 25 spuštěních virus zahájil mazání disku
- objevilo se několik programů, které bojovaly proti tomuto viru, dokázaly jej odhalit

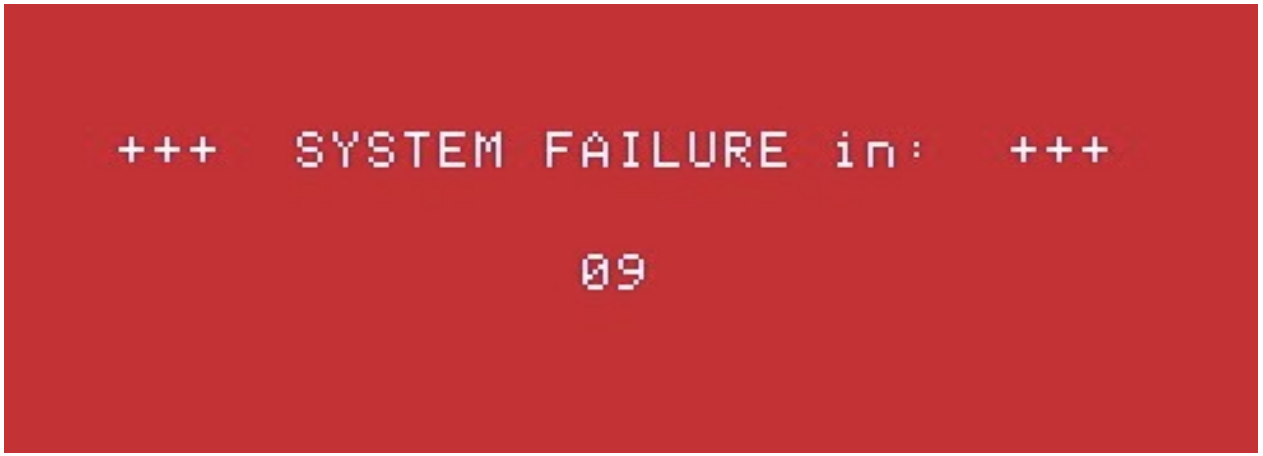

[WOP] -666- FESTERING HATE -666- [FOG]
The Good News: You now have a copy of one of the greatest programs that has ever been created!
The Bad News: It's quite likely that it's the only program you now have in your possession.
Hey Glen! We sincerely hope our royalty checks are in the mail! Seeing how we're making you rich by providing a market for virus detection software!
Elect LORD DIGITAL as God committee!
)/> The Kool/Rad Alliance! <\(
Rancid Grapefruit -- Cereal Killer
This program is made possible by a grant from Pig's Knuckle ELITE Research. Orderline: 313/534-1466
[(C) 1988 ELECTRONIC ARTS]
Worshippers of Patrick
Friends of Glen Bredon

- Jméno tvůrce viru Lord Digital patří Patricku Karlu Kroupovi slavnému hackerovi, který prošel mnoha významnými hackerskými skupinami v 80. letech

- patří k první generaci, která již od dětských let vyrůstala s osobnímimi počítači
- Patřil do první skupiny hackerů pro počítače Apple
- společně s dalšími založil slavnou hackerskou skupinu – Legion of Doom (1984)
- v 80.letech člen kontrakulturního hnutí, jež se scházelo v New Yorku,

- V 90. Letech vstoupil do mainstreamu svou esejí o počátcích a budoucnosti kyberprostoru
- Voices in my Head, MindVox: The Overture
- stal se známou osobností, mytologii kyberprostoru rozvíjí v časopisu Wired
- Bral velmi dlouho drogy, závislost na heroinu

- Virus Load Runner (1989) – varovné hlášení



- Virus Blackout (1989) – kompletní ztišení počítače, černé pozadí

- apple problém virů nijak neřešil
- v této době komunita kolem počítačů Apple založena na vzájemné dvěře
- Po roce 89 přesun hackerů na jiné počítače Amiga, PC, Atari ST

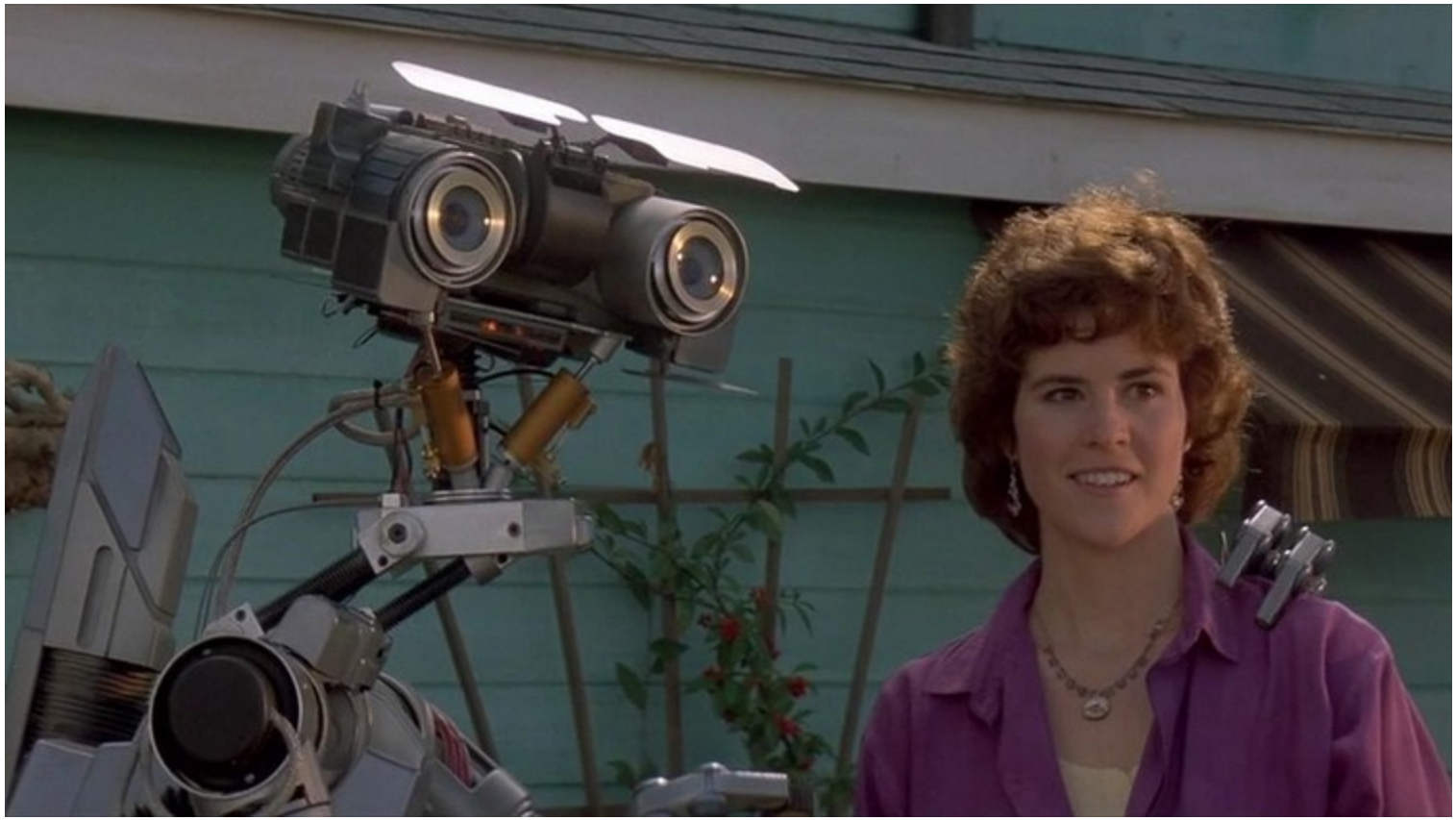
Viry na počítači Amiga (1985) – praktická realizace myšlenky počítačového viru v Evropě

- Uvedení Amigy v roce 1985
- Tvorba virů předmětem undergroundové počítačové kultury zejména v Evropě
- Charakteristické vlastnosti těchto komunit – technologické nadšení, amorálnost, chaotičnost, kreativita

- Nejznámější skupiny: Byte Bandits, Swiss Cracking Association
- První virus – SCA Virus (1987) –
- když infikoval počítač napsal následující sdělení - https://www.youtube.com/watch?v=bac84Ibo_y4
-

- Virus SCA využíval boot sector na disku o velikosti 1024 bytů kódu
- při spuštění disku se nejdříve spustil kód viru a nakopíroval se do paměti, pak se spustil správný kus kódu
- SCA virus neměl za úkol poškodit počítač
- Hlavním úkolem dokázat, že je možné napsat program tohoto druhu

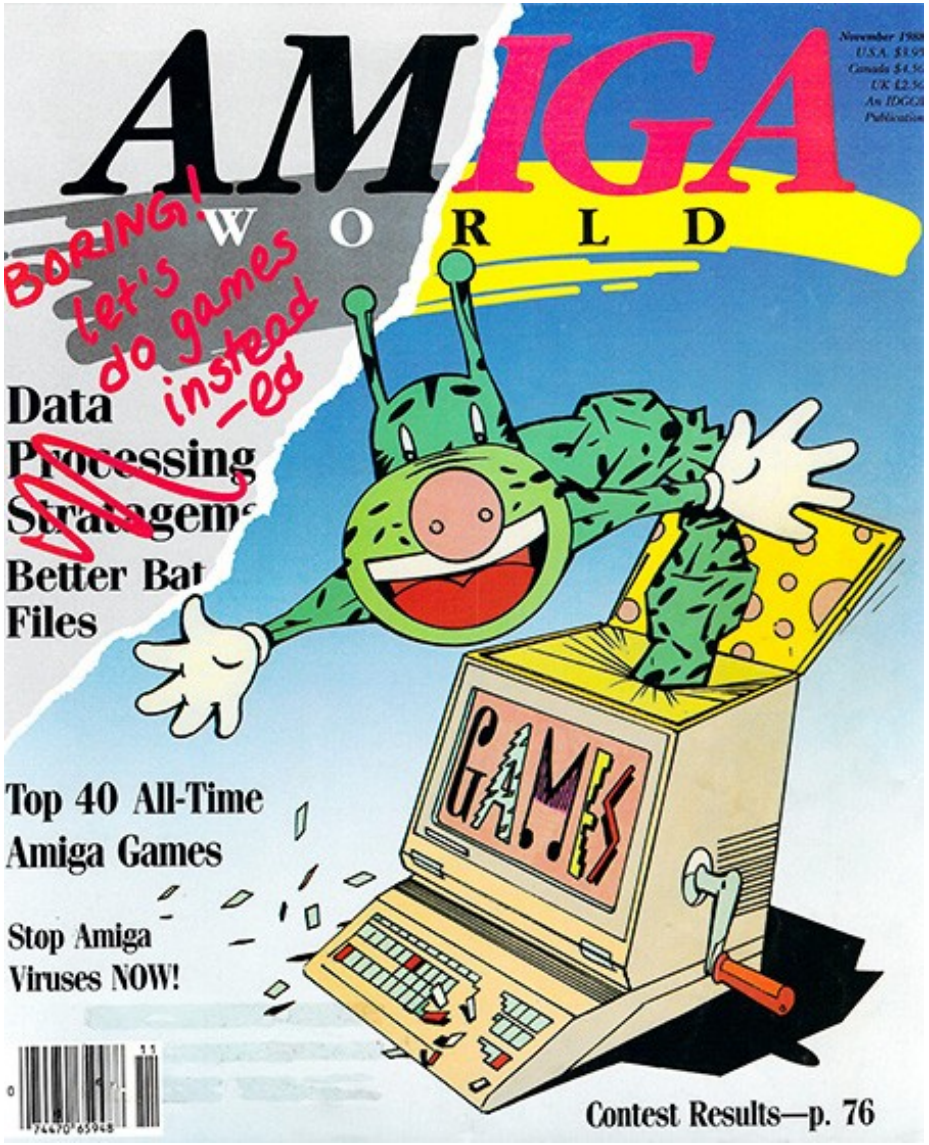
- Věta: „Something wonderful has happened…“ inspirována tímto filmem



- Virus od hackera ze skupiny Byte Bandit - zčernání obrazovky a zaseknutí počítače¨, nutné napsat tajný kód
- Lamer Exterminator (1989) - přepisoval náhodné sektory na disku slovem Lamer!
- Saddam Hussein (1991)

- Právě v roce 1987 se objevilo větší množství virů i na ostatní platformy, začalo se uvažovat o jejich nebezpečnosti
- Zaměstnanec firmy Commodore Bill Coester přidělen na výzkum virů, úkol: zajistit jejich eliminaci
- Commodore začal uvažovat o virech jako o problému
- Varování časopisu AmigaWorld (1988)

Amiga World Vol 04 11 1988



Tvorba virů ve vědeckém prostředí

- Fred Cohen – jeden z prvních vědců, který se zabýval viry a jejich nebezpečným potenciálem
- pokusil se vyvinout experimentální počítačový virus, aby dokázal, že se jedná o nový typ hrozby
- 3.11.1983 - vypuštěn první experimentální virus na týdenním semináři počítačové bezpečnosti
- Různá bezpečnostní opatření, virus byl pod kontrolou
- Měřena rychlost útoků viru, rychlost je překvapila nejvyšší rychlost pod ½ sekundy

Takeover 1:

Elapsed Time	Event	Effect
0	Program announced on BBoard	existence published
3 min	Administrator runs program	system utility infected
5 min	root executes utility	All privileges granted

Takeover 2:

Elapsed Time	Event	Effect
0	Program announced on BBoard	existence published
1 min	Social user runs program "loadavg"	infected
4 min	Editor owner runs "loadavg"	Editor infected

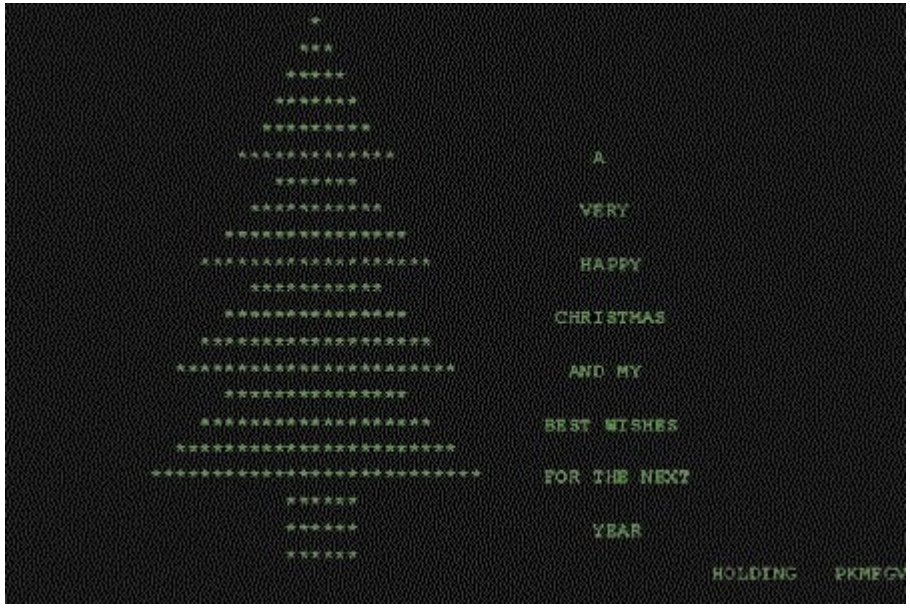
- Jakmile byly výsledky experimentu zveřejněny, administrátoři zakázali další experimenty na jejich systému (UNIX)
- Vedoucí počítačové bezpečnosti nepovolil další experimenty
- Březen 1984 další experiment – virus na Bell – LaPadula systému
- Virus dokázal překročit uživatelské privilegie a pohybovat z nižší úrovně zabezpečení do vyšší úrovně

- Raná 80. léta návrat Core Wars (A. K. Dewdney) –
- od roku 1986 pravidelné soutěže
- Software volně ke stažení
- Ukázka: https://www.youtube.com/watch?v=-ytlji6T8R0

Negativizace viru (druhá pol. 80. let)

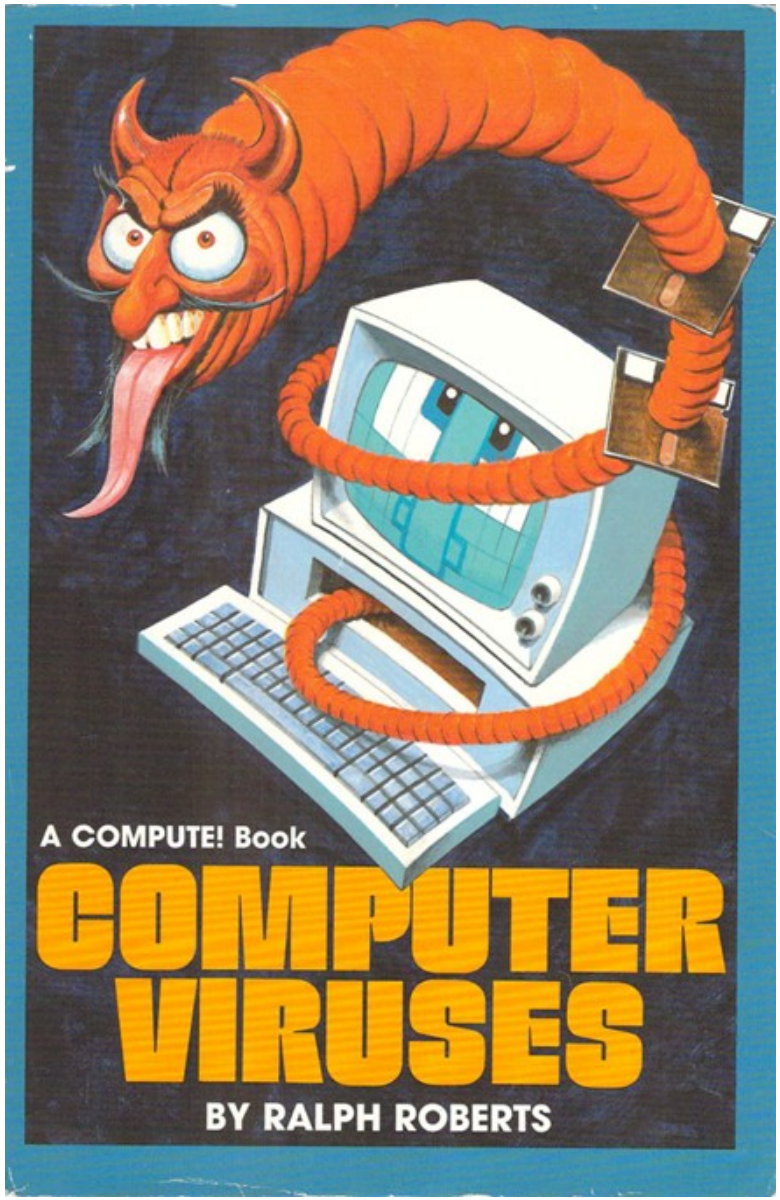
- 1984 - Virus hlavním tématem prezentace Freda Cohena na konferenci o počítačové bezpečnosti
- 1985 - první článek o počítačových virech v magazínu Times
- Brain virus (1986) – první PC virus – infikoval soubory s příponou exe a com – https://www.youtube.com/watch?v=lnedOWfPKT0
- 1987 - Virus Lehigh –dostal se do širšího povědomí, protože mazal celý disk

- Email worm CHRISTMA EXEC pro IBM střediskové počítače - šířil se prostřednictvím emailu



- V roce 1987 uspořádal Christopher Langton první konferenci věnovanou tematice umělého života, která se konala v Los Alamos
- Langton vyloučil z konference jakékoliv příspěvky týkající se počítačových virů, až na jedinou výjimku: A Core War Bestiary of Viruses, Worms and Other Threats to Computer Memories

- Jeruzalem virus – destruktivní náklad, autor Yisrael Radai,
- Edice - COMPUTE! Book - Computer Viruses – Ralph Roberts


A COMPUTE! Book
COMPUTER VIRUSES
BY RALPH ROBERTS

Morris Worm – mediální virus

- Tvůrce student Robert Morris
- Kvůli chybě v programování počítačový červ unikl
- Škody ve výši 10 000 000 dolarů
- Využíval chyby v síti, šířil se ranou verzí internetu
- Tento případ široce medializován

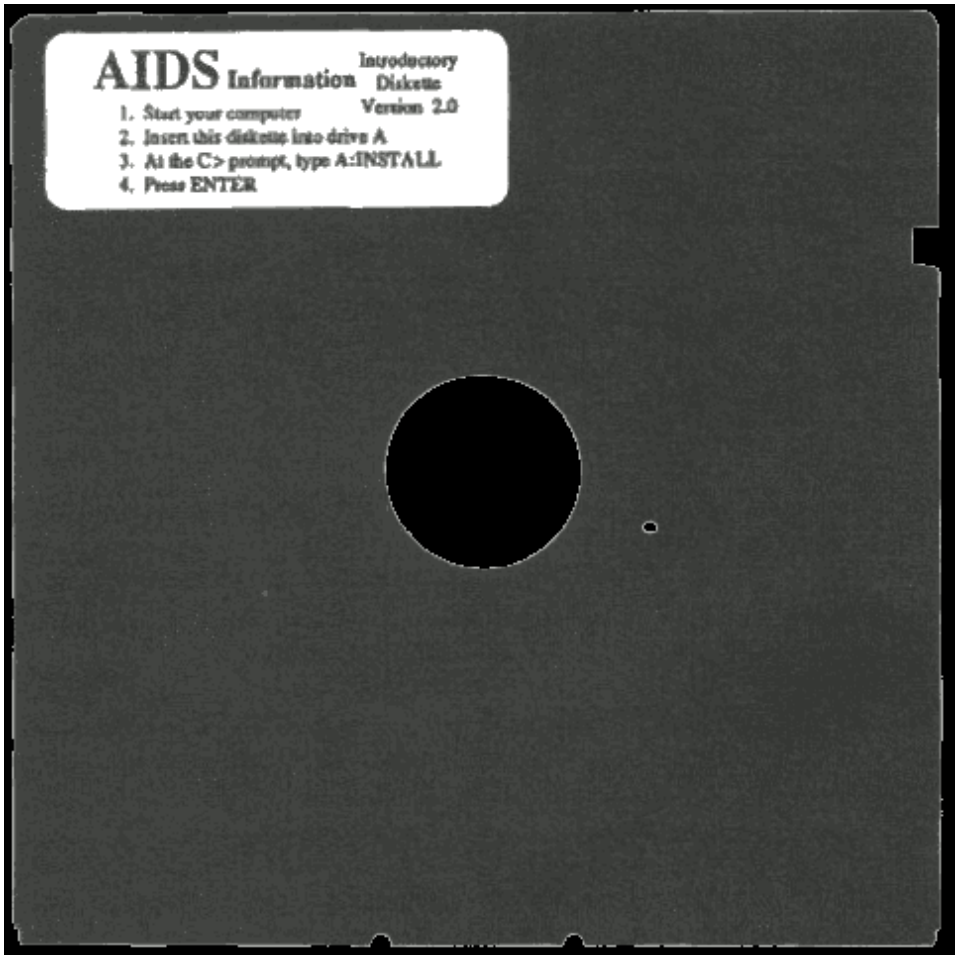
- Morris Worm určil způsoby, kterými bude prezentován virus v médiích

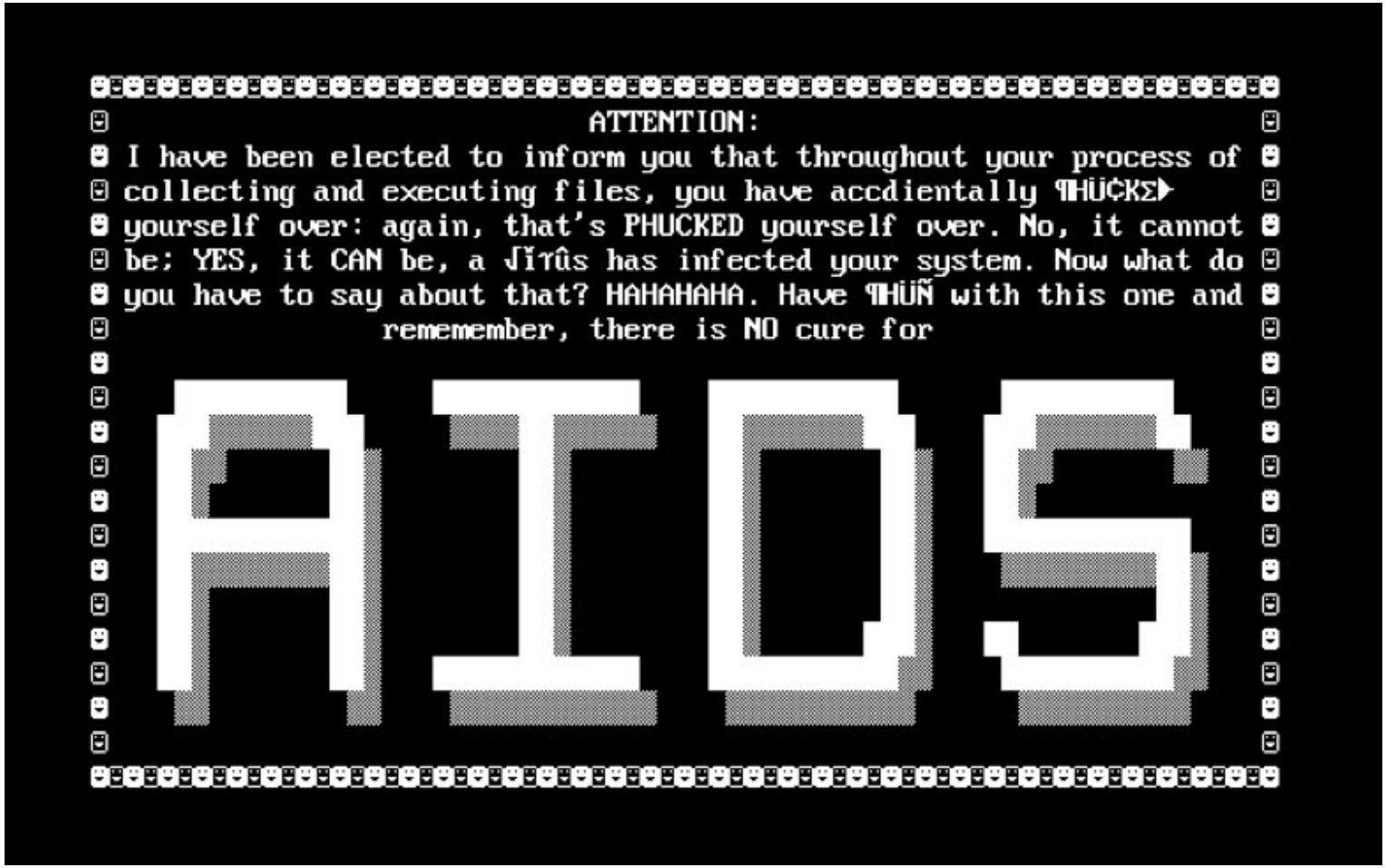
- Morris byl za svůj čin odsouzen ke 400 hodinám veřejných prací

- Počítačový červ upozornil na zranitelnost internetové sítě -vznik institutu CERT (1988)

- Morris Worm se stal důležitou součástí historie digitální kultury, uložen v Muzeu počítačové historie

AIDS Trojan (1989)




ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accdientally ¶HÜ¢KΣ►
yourself over: again, that's PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a √ĭτûs has infected your system. Now what do
you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
rememember, there is NO cure for
AIDS

90. léta – Nové formy virů, rychlé šíření skrze internet

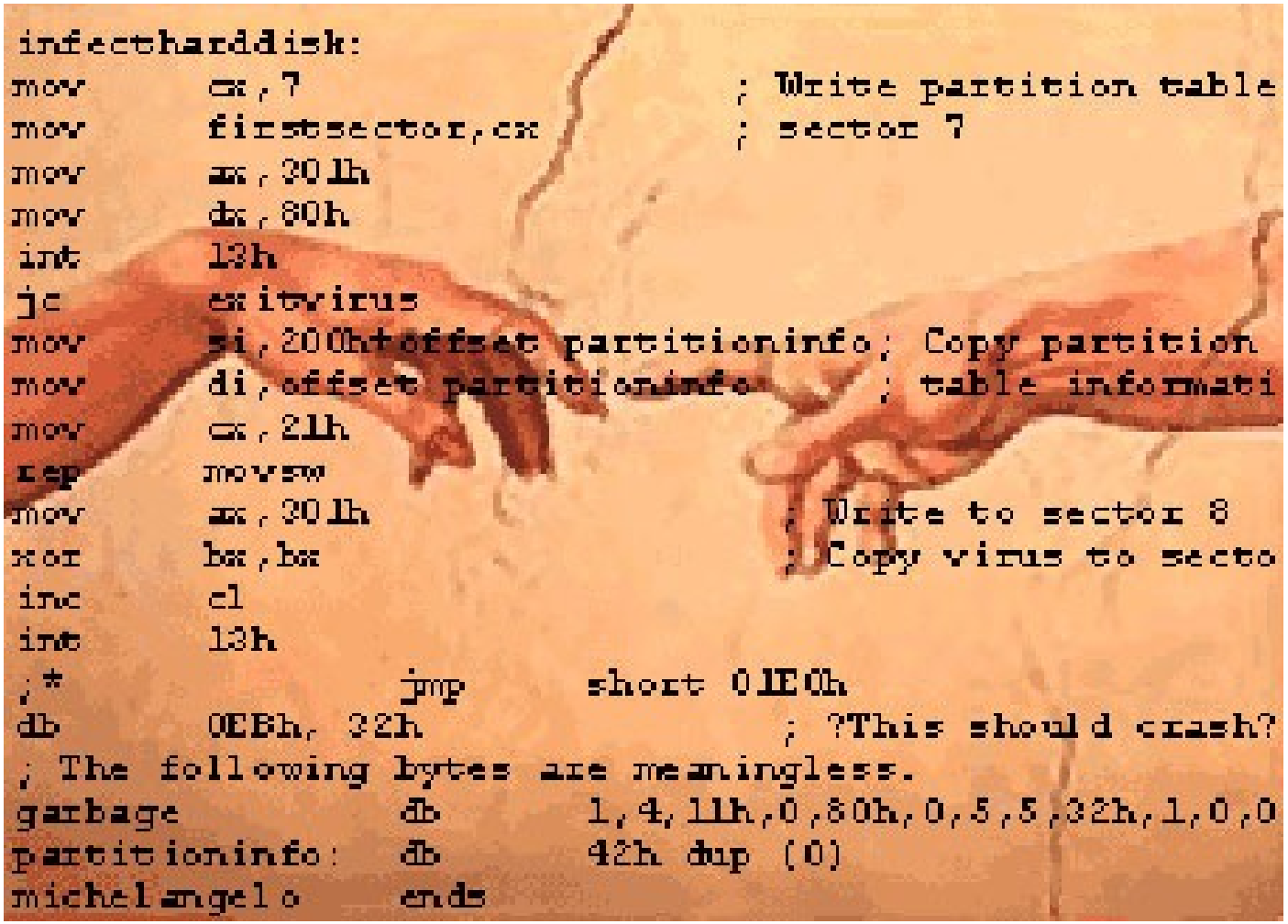
- **Nové viry**
- Polymorfní
- mnohostranné viry (multipartite virus) –
- stealth viry - viry, které se dokáží maskovat v systému – virus Frodo

- obliba virtuálních bulletinů - Virus-exchange boards – komunikační platforma pro tvůrce virů
- Centrem tvorby virů – Bulharsko, Rusko

- 1991- konstrukční soupravy pro tvorbu virů

- 1992 – Generátory virů

Michelangelo virus (1992)

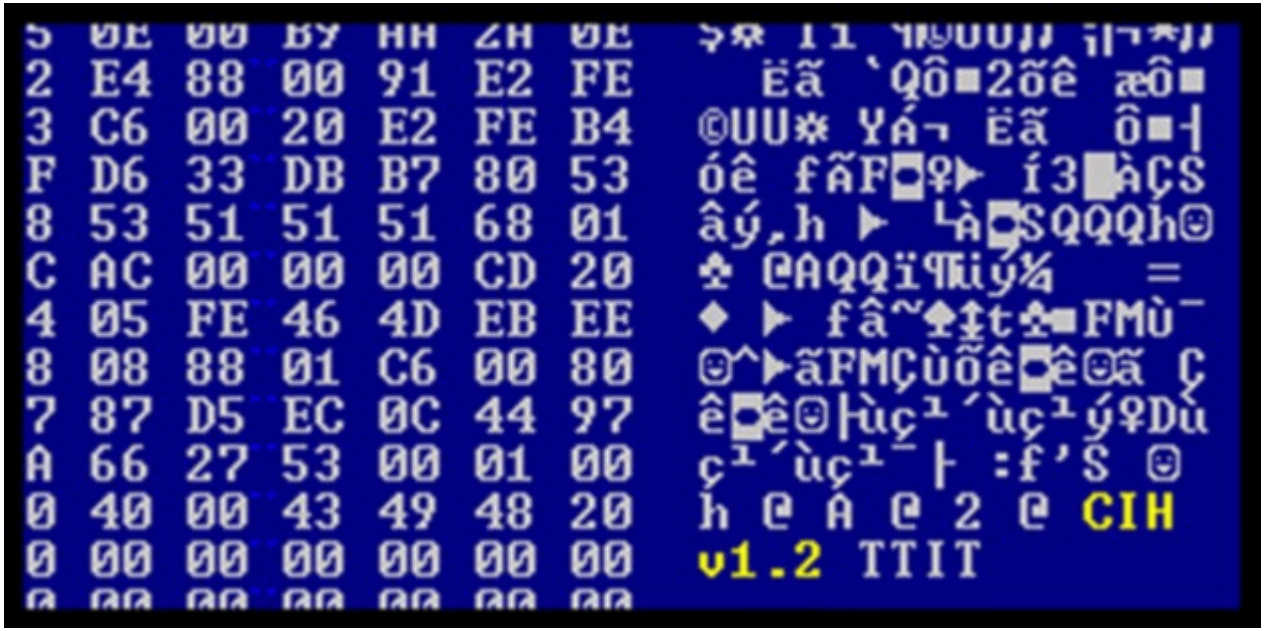


```
infectharddisk:
mov     cx,7                    ; Write partition table
mov     firstsector,cx          ; sector 7
mov     ax,201h
mov     dx,80h
int     13h
jc      exitvirus
mov     si,200h+offset partitioninfo; Copy partition
mov     di,offset partitioninfo     ; table informati
mov     cx,21h
rep     movsw
mov     ax,201h                   ; Write to sector 8
xor     bx,bx                     ; Copy virus to secto
inc     cl
int     13h
;*              jmp     short 0EC0h
db      0EBh, 32h                       ; ?This should crash?
; The following bytes are meaningless.
garbage         db      1,4,11h,0,80h,0,5,5,32h,1,0,0
partitioninfo:  db      42h dup (0)
michelangelo    ends
```

One_Half.3544.A.

- Vytvořen na Slovensku
- polymorfní a multipartitní virus
- Chytré maskování před všemi tehdejšími antiviry

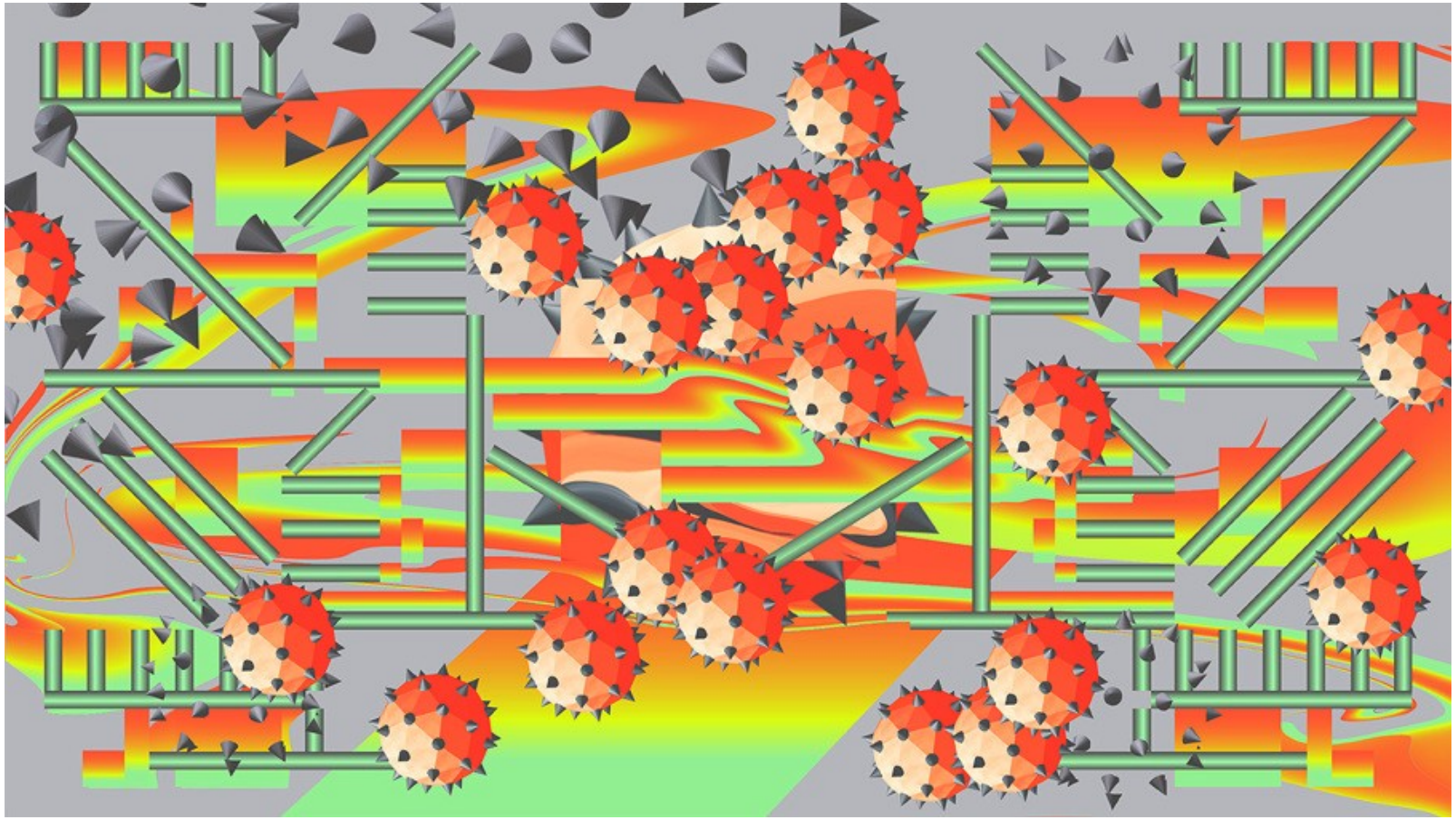
Černobyl (1998)



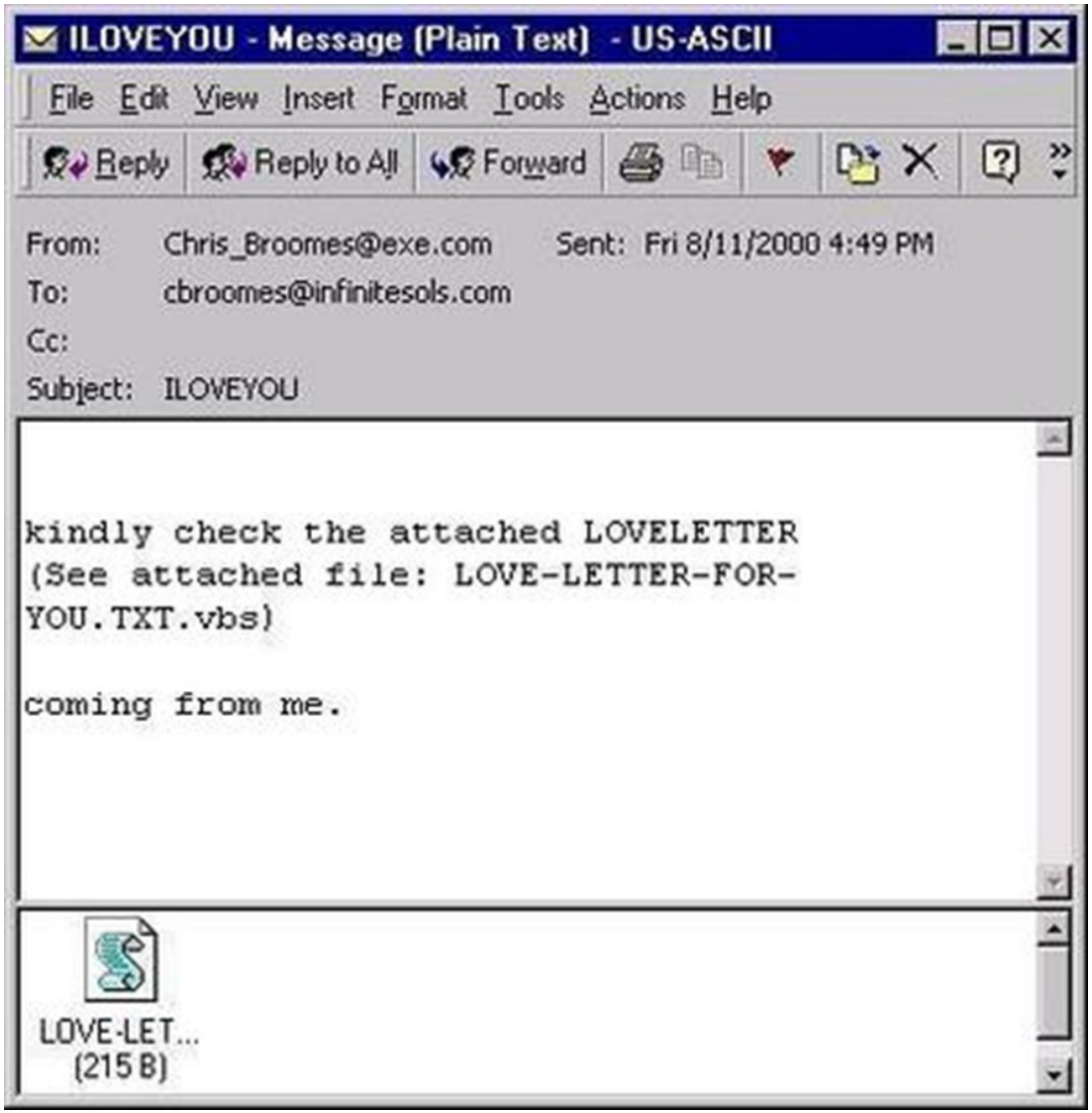
Solar Sunrise (1998)

- Virus, který ovládl zhruba 500 vládních vojenských systémů
- Pro operační systém SunSolaris
- Incident byl původně připisován íránským vládním hackerům
- Brzy se ale přišlo na to, že autory viru byli dva Američané

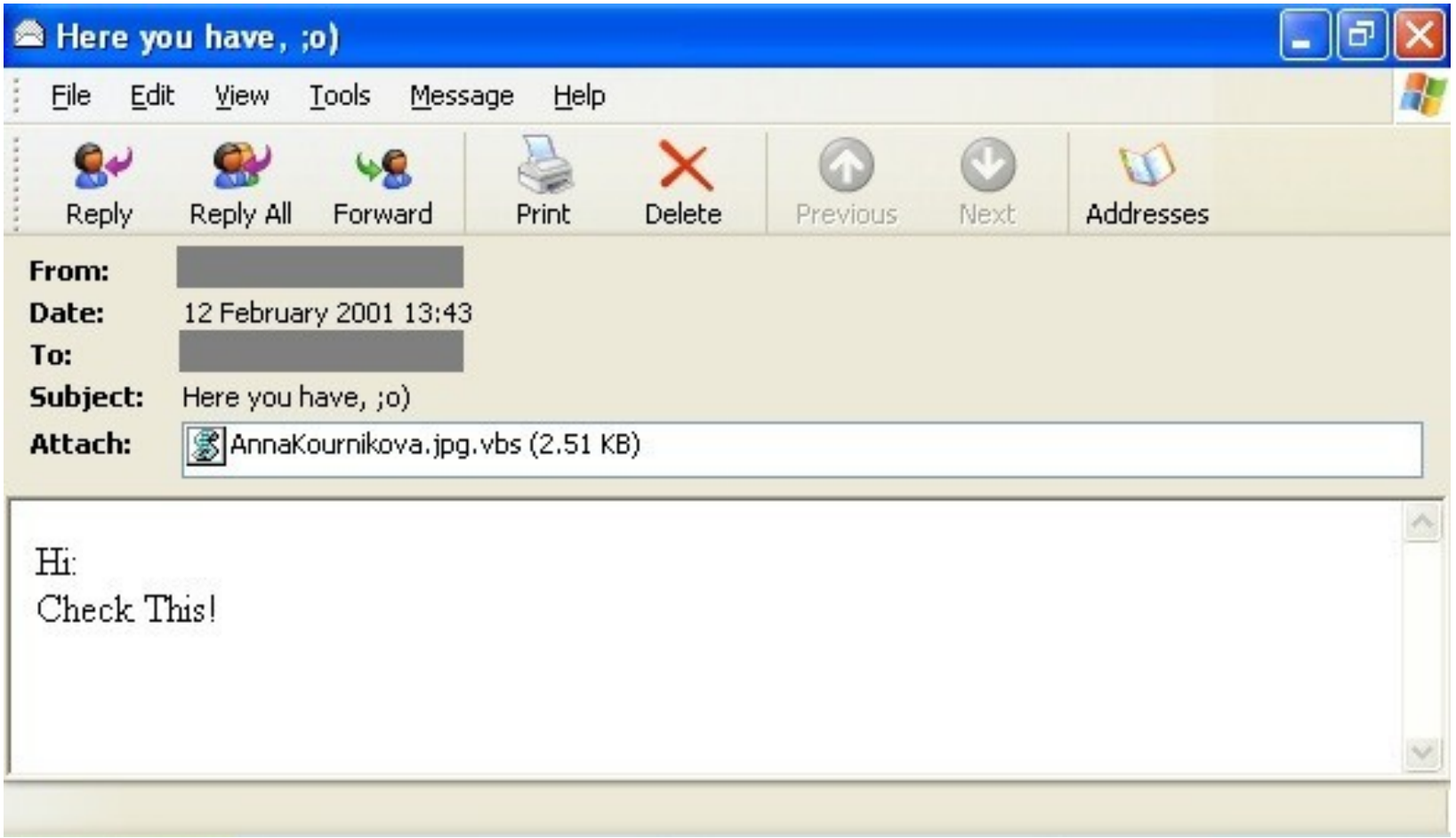
2000 – 2010 - Období makrovirů, backdoor viry, DoS útoky



I love you (2000)



ANNA KOURNIKOVA



MyDoom (2004)

- Šíří se pomocí e-mailů ve formě přílohy
- Když je virus vypuštěn zavede do počítače backdoor, který otevře porty pro přístup na internet
- Umožňuje tak útočníkovi přístup k souborům počítače
- Odhaduje se, že zasáhl 20 až 30 procent všech počítačů

SpamTool.Win32.Small.b

- Virus, který vnikl do počítače a sbíral zde adresy, které posílal tvůrci viru
- Poté na ně mohl posílat nevyžádanou poštu
- phishing – emaily, které žádají po uživateli číslo kreditní karty
- Mohl obchodovat se seznamem adres

od 2010 - Špionážní viry, Ransomware

Stuxnet (2010)

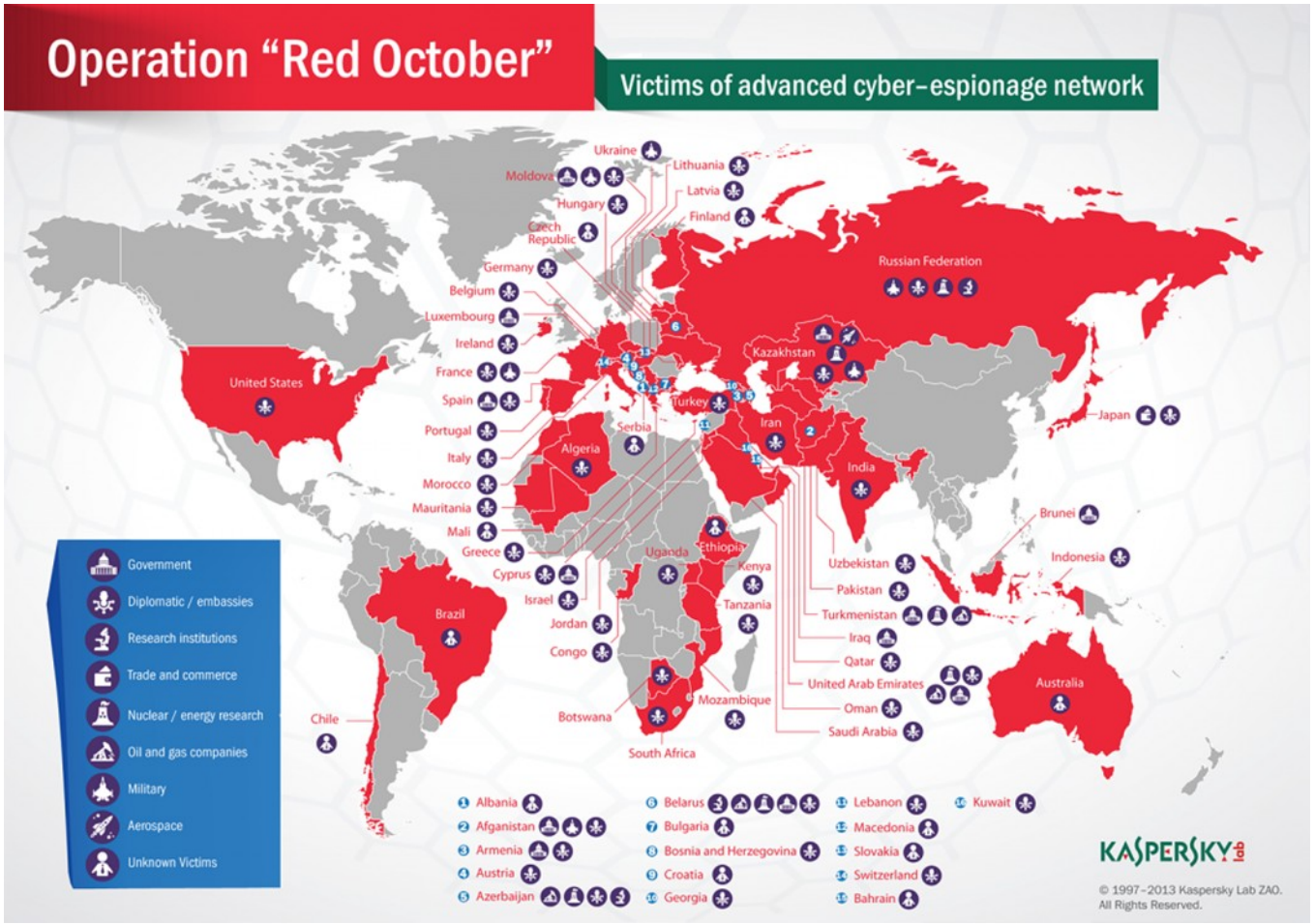
- Infikoval průmyslový software firmy Siemens
- Hlavním cílem viru byly různé průmyslové objekty na území Íránu
- Šířil se prostřednictvím USB disků
- nejspíše se jednalo o armádní projekt, který vznikl buď na území Izraele nebo USA

- https://www.youtube.com/watch?v=DSMOs7CF1Eo

Flame (2012)

- využíván pro špionáž na středním východě
- sbírá data nejrůznějšího druhu
- zasaženo přibližně 1000 počítačů
- podporuje tzv. kill command, který vymaže veškeré stopy viru
- Původ v tajných službách a armádě
- Velmi sofistikovaný

Operace Rudý říjen - 2013



Policejní virus (Švédsko) - 2016

Policejní virus (ČR) - 2016