Virus v diskurzu nových médií

Adam Franc

Způsob ukončení předmětu

- Písemný test
- 10 otázek uzavřených (výběr z možností)
- 2 otázky otevřené
- 1 otázka bonusová (kreativní úkol)

Osnova

- 1. Úvodní hodina – obsah a průběh kurzu, způsob ukončení, doporučená literatura, definice biologického a počítačového viru, historický vývoj počítačového viru, současné (počítačové) viry
- 2. Filozofické myšlení o viru - Gilles Deleuze, Felix Guattari, Michel Serres, Bruno Latour, Actor-Network Theory
- 3. Tři dominantní způsoby myšlení o viru - virus jako umělý život, virus jako metafora, virus jako řečový akt
- 4. Umělecký potenciál viru, reprezentace viru v populární kultuře, pozitivní virus

Literatura

- Parikka, Jussi. Digital Contagions: A Media Archaeology of Computer Viruses. New York: Peter Lang Publishing, 2007.
- Franc, Adam. Virus jako předmět výzkumu v diskurzu nových médií. Diplomová práce. Masarykova univerzita, Filozofická fakulta, 2014.
- Dibbell, Julian. Viruses Are Good for You. Wired, roč. 3, č.2, 1995.
- Sampson, D., Tony - Parikka, Jussi (eds.). The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture. Cresskill: Hampton Press, 2009.
- Latour, Bruno. Nikdy sme neboli moderní. Bratislava: Kalligram, 2003.
- Thomas, Anne-Marie. It Came from Outer Space: The Virus, Cultural Anxiety and Speculative Fiction. PhD Thesis. Louisiana State University, 2002.

Vzájemné ovlivňování biologie a digitální kultury

- Tvorba analogií mezi biologickým a technologickým
- Tyto analogie do značné míry určují, jakým způsobem chápeme digitální kulturu, tělesnost apod.

Příklady:

- zakládající analogie mezi neurony a počítačovými komponenty
- přirovnání dna k softwaru

- Biologické organismy jako metafory pro počítačové viry
- Virus představuje základ logiky digitální kultury
- Hlavní vlastnosti: konektivita, samoreprodukce, kopírování, mutace, aktualizace, komunikace, interakce, autonomie, kooperace
- Virus jako přirozený obyvatel digitální ekologie

Definice biologického viru

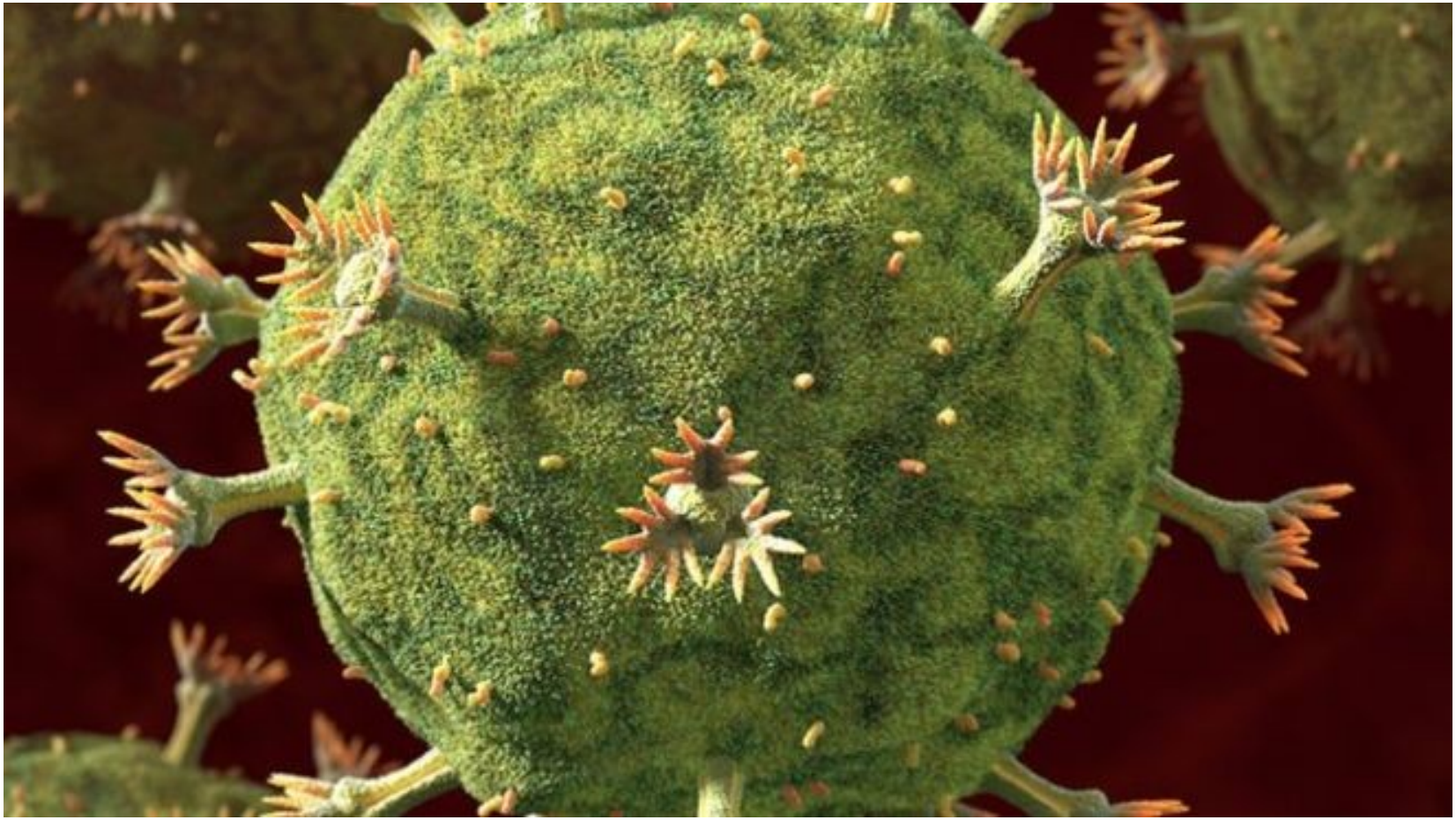
- Slovo virus v latině znamená jed
- Jednoduchý organismus, který se nemůže rozmnožovat, růst ani vytvářet energii bez hostitelského organismu

Obvyklý průběh infekce

- a) Přilnutí viru na povrch buňky
- b) Vniknutí viru do buňky
- c) Replikace viru

- Tento proces, ale může mít několik scénářů, které závisí na druhu viru:
- 1. Virus přepíše genetický kód buňky
- 2. existuje v buňce bez toho, aniž by narušil její fungování,
- 3. využije ji ke své replikaci
- 4. nebo se stane součástí její DNA.

Příklad - Virus HIV



- Virus imunitní nedostatečnosti - oslabuje imunitní systém
- s oslabováním imunitního systému se rozvíjí AIDS (získaný syndrom imunitní nedostatečnosti)
- Začlení se do genomu hostitelské buňky, kde je skryt před imunitním systémem
- první případy popsány v roce 1981

- teorie vzniku - Existuje více teorií vzniku viru HIV. Zde jsou některé z nich:
- 1) Mutace viru – virus existoval u člověka už od pradávna, ale v současné době díky okolnímu prostředí a stylu života zmutoval
- 2) Přenos z opic – opírá se o podobnost viru HIV s virem SIV, který mají opice, virus se postupně adaptoval na člověka

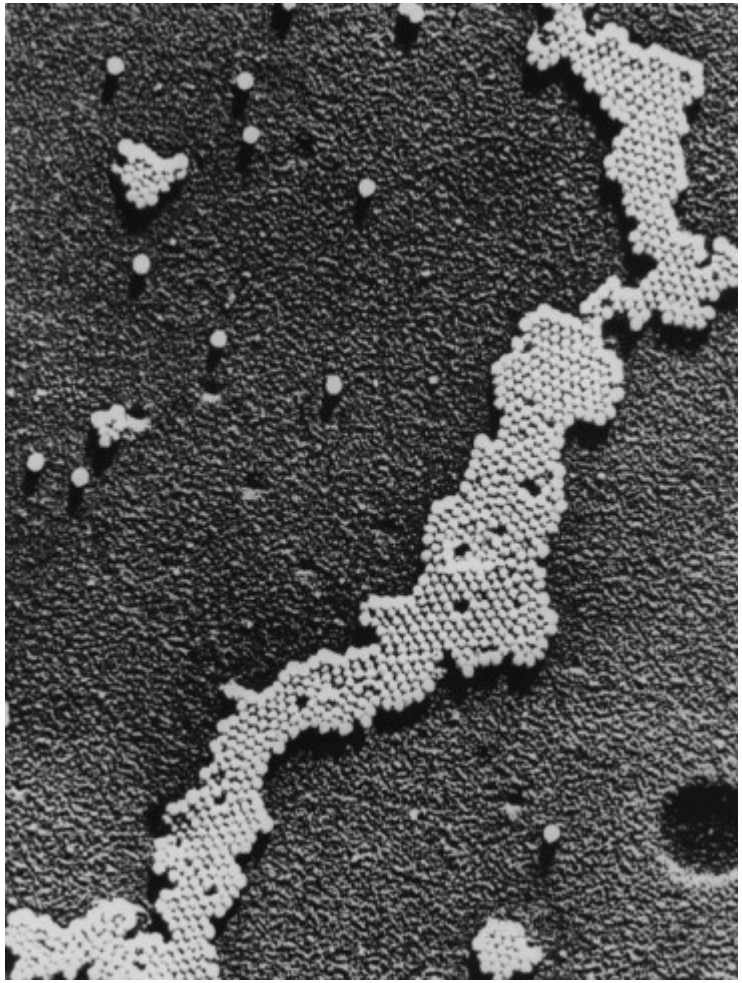
Příklad prospěšného viru - Bakteriofágy

- léčba bakteriálních infekcí,
- ničí škodlivé bakterie, jež nám mohou způsobit různá onemocnění
- napadá pouze bakteriální buňky.
- prostředek pro zničení rezistentních druhů bakterií

Historie objevu viru

- Až do konce devatenáctého století byly infekce přisuzovány bakteriím a o existenci něčeho menšího se nevědělo.
- pokus s extrakty z tabáku napadeného tzv. tabákovou mozaikou - Dmitrij Ivanovskij (1892)
- Viry jako živoucí kapalina - Martinus Beijerinck zopakoval tyto pokusy (1898), tvrdil, že existuje nakažená kapalina

- 1931- Eli Franklin Burton na Torontské univerzitě vynalezl první elektronový mikroskop zvětšoval 400x
- Objevil se první obraz viru:



Virus – živý x neživý?

- Virus nezapadá do zavedené definice života
- nevytváří energii a tedy nemají metabolismus
- Viry nerostou
- Na druhou stranu někteří považují virus za živý, když vnikne do buňky a začne využívat její systémy
- Další názor: z hlediska funkce a významu do stromu života patří, významně ovlivňují vývoj všech druhů ne zemi, přepisování DNA, součást ekosystému

Počítačový virus – základní dělení

- Definice (technologická) - virus je schopen sebe-replikace, tedy množení sebe sama, ovšem za přítomnosti hostitele, k němuž je připojen
- Nejrozšířenější definice počítačového viru vychází z díla Freda Cohena - badatel, který se zabývá výzkumem počítačových virů již od 80. let minulého století.
- „**Virus je program, který může infikovat jiné programy tím, že je modifikuje, aby do nich mohl zahrnout identickou, případně rozvinutou, kopii sebe sama.**“

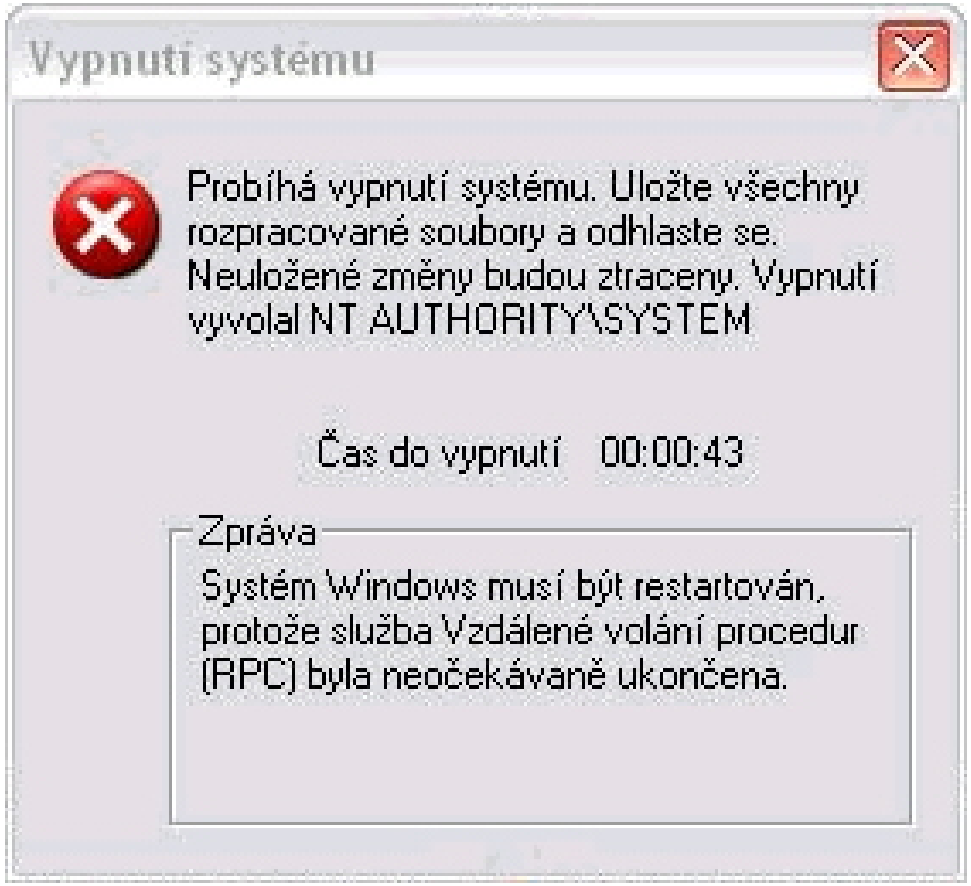
Definice společnosti Microsoft

- „Počítačové viry jsou malé softwarové programy, které jsou určeny k tomu, aby se rozšiřovaly od jednoho počítače k druhému a narušovaly jeho operace. Počítačový virus může poškodit nebo vymazat data na tvém počítači, využít tvůj emailový program ke svému šíření do dalších počítačů nebo dokonce vymazat všechna data uložená na tvém pevném disku.“

Druhy malwaru

- počítačový virus často zaměňován s podobnými typy programů, které však fungují odlišně,
- pro pojmenování různých druhů škodlivého softwaru se užívá souhrnný název malware
- malware je zkratkou slovního spojení Malicious Software, které lze přeložit jako škodlivý nebo se zlým úmyslem šířený software.

- Trojské koně – Password stealing trojan, destruktivní trojan , Proxy Trojan
- Počítačový červ – příklad-Lovsan/Blaster



- Spyware
- Hoax – příklady – Olympic torch, MusicPanel

Syntetické viry vytvořené člověkem – mezi digitálním a biologickým

- Poliovirus vytvořený člověkem - poliovirus jednoduchý RNA virus složený ze 7741 bází, syntetizovali jeho genom
- Vědci ze Státní university v New Yorku (Jeronimo Cello, Aniko Paul a Eckard Wimmer)
- když vložili RNA do samčích buněk, virus začal pracovat, první replikující se organismus vytvořený lidskou rukou

Mycoplasma mycoides JCVI-syn1.0 (2010)

- J. Craig Venter Institute – vědci zmapovali kompletní DNA bakterie a převedli její genom na vlastní abecedu, kterou uložili do počítače
- DNA modifikovali a syntetizovali vlastní genom a transplantovali jej do jiné bakteriální buňky
- nová buňka začala být řízena výhradně touto DNA

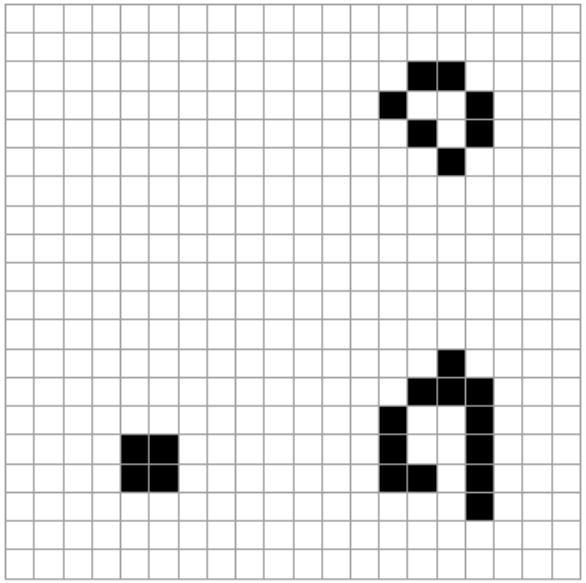
Genová abeceda

TAG = a	GCA = k	TCC = u	AGA = 4	CAC = /
AGT = b	AAC = l	TTG = v	GCG = 5	CCA = =
TTT = c	CAA = m	GTC = w	GCC = 6	CGA = .
ATT = d	TGC = n	GGT = x	TAT = 7	GAG = !
TAA = e	CGT = o	CAT = y	CGC = 8	CAG = :
GGC = f	ACA = p	TGG = z	GTA = 9	GGA = "
TAC = g	TTA = q	TCT = 0	ATA = space	GTG = ,
TCA = h	CTA = r	CTT = 1	GGG = chr(10)	TCG = @
CTG = i	GCT = s	ACT = 2	AGC = >	CCC = -
GTT = j	TGA = t	AAT = 3	CGG = <	

- Informace vložené do dna
- Tři citáty - TO LIVE, TO ERR, TO FALL, TO TRIUMPH, TO RECREATE LIFE OUT OF LIFE." - JAMES JOYCE; "SEE THINGS NOT AS THEY ARE, BUT AS THEY MIGHT BE."-A quote from the book, "American Prometheus"; "WHAT I CANNOT BUILD, I CANNOT UNDERSTAND." - RICHARD FEYNMAN.

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

- John von Neumann - Idea replikace
- myšlenka celulárního automatu, který reprodukuje sám sebe – článek - Theory of Self-Reproducing Automata



- 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)

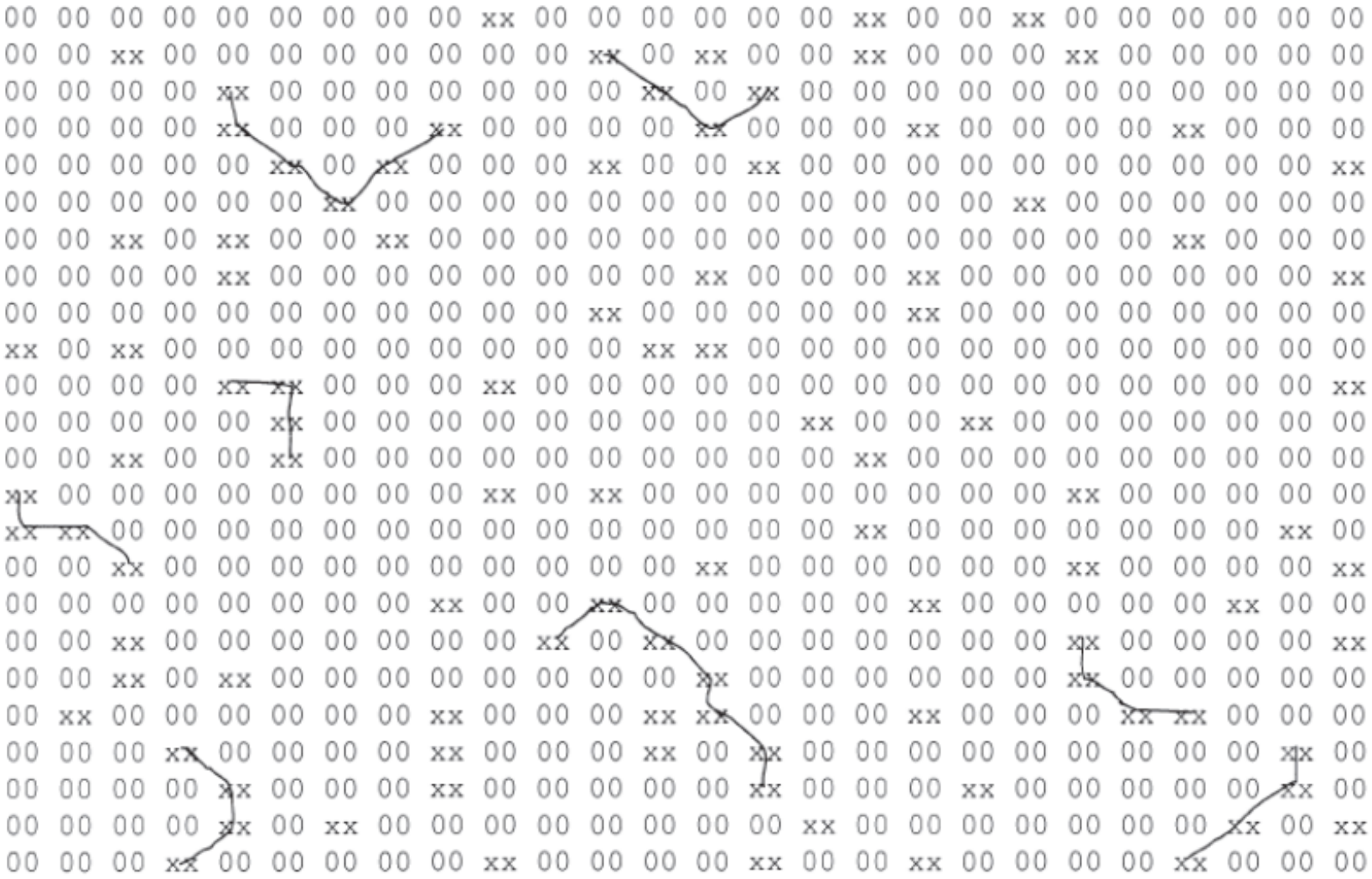
Game of life na Atari 2600 - https://www.youtube.com/watch?v=bSWhDHybXDY

Von Neumannova architektura

- 1. operační paměť
- 2. aritmeticko-logická jednotka
- 3. řadič – řídicí jednotka
- 4. vstupní zařízení
- 5. výstupní zařízení
- vnitřní struktura počítače by se neměla nijak měnit v závislosti na zpracovávané úloze, měla by být univerzální
- programy i data se uchovávají v téže operační paměti

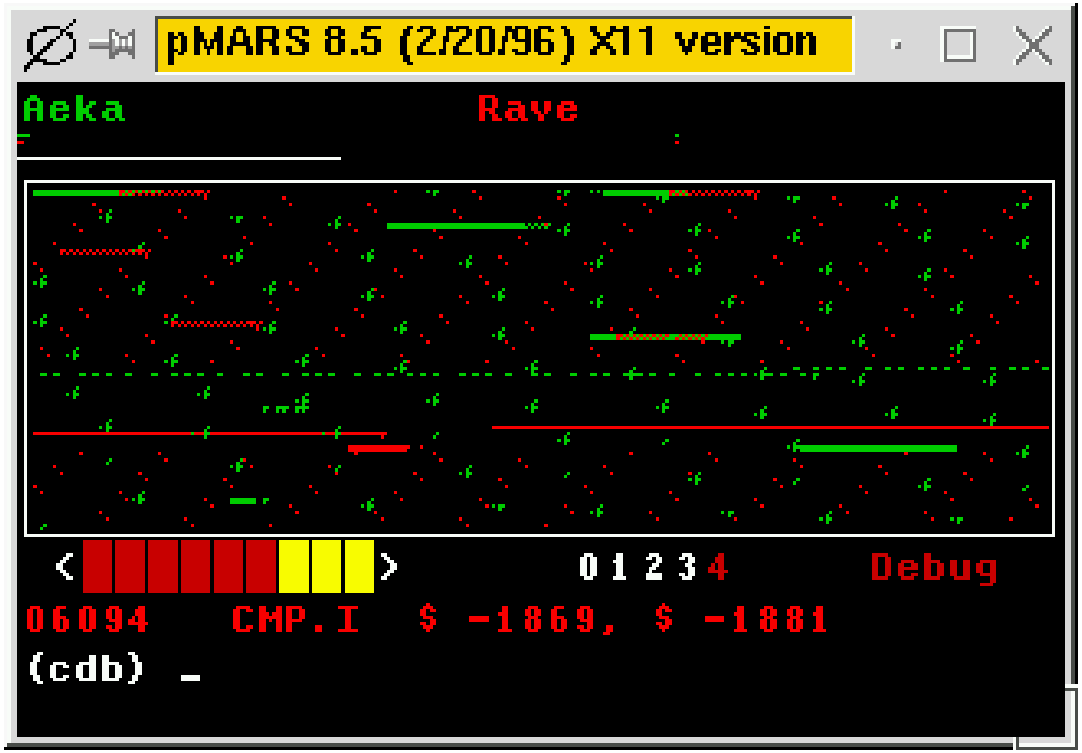
- programy podobné virům byly označovány jako červy – programy, jež narušovaly osobní prostor jiných programů, často produkovaly náhodné operace a chyby - důsledek této architektury
- kdybychom se pokusili sledovat stopu chybných operací odhalili bychom náhodné vzory paměťových lokací, v podobě nepravidelných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

Wormhole damage pattern



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

- Core wars (od 1961) – vytváření virů jako sport, kdo udělá lepší program, který zničí ostatní



- 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

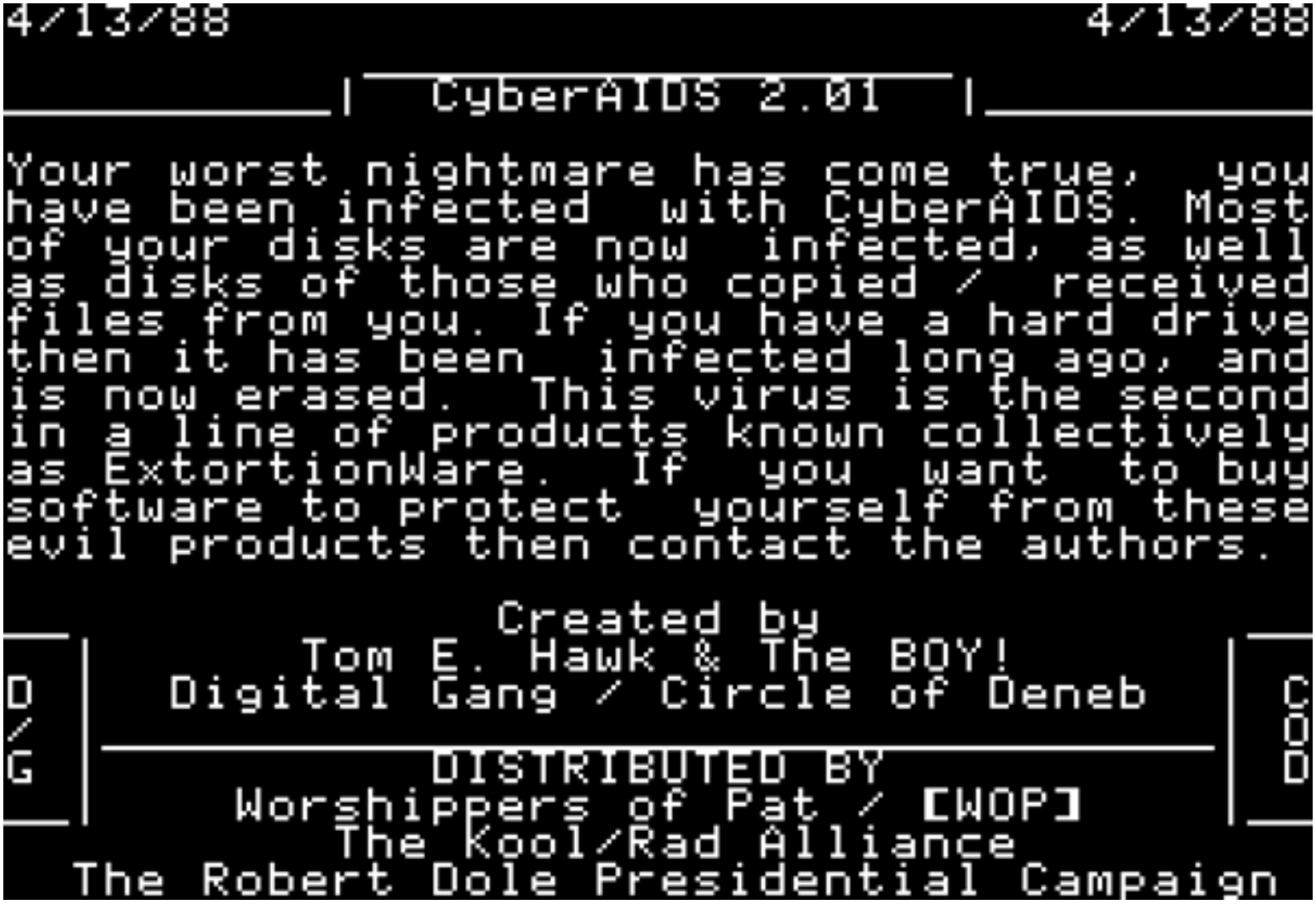
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

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, šířil se prostřednictvím BBS fóra, využíval telekomunikační program Zlink, virus přenášen přes ranou verzi internetu
- 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 - pirátské kopie her, prolomení ochrany, hackování telefonů
- Poté společně s dalšími založil slavnou hackerskou skupinu – Legion of Doom (1984)
- v 80.letech člen kontrakulturního hnutí, jež se scházelo v New Yorku, změnilo jeho pohled na úlohu technologií

- 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

- apple problém virů nijak neřešil, neboť se neprojevoval v tak velkém měřítku, vždy se snažili pouze vytvořit lék na virus, ale nezaměřovali se na prevenci hrozby nebo pronásledování hackerů
- Po roce 89 přesun hackerů na jiné počítače Amiga, PC, Atari ST

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

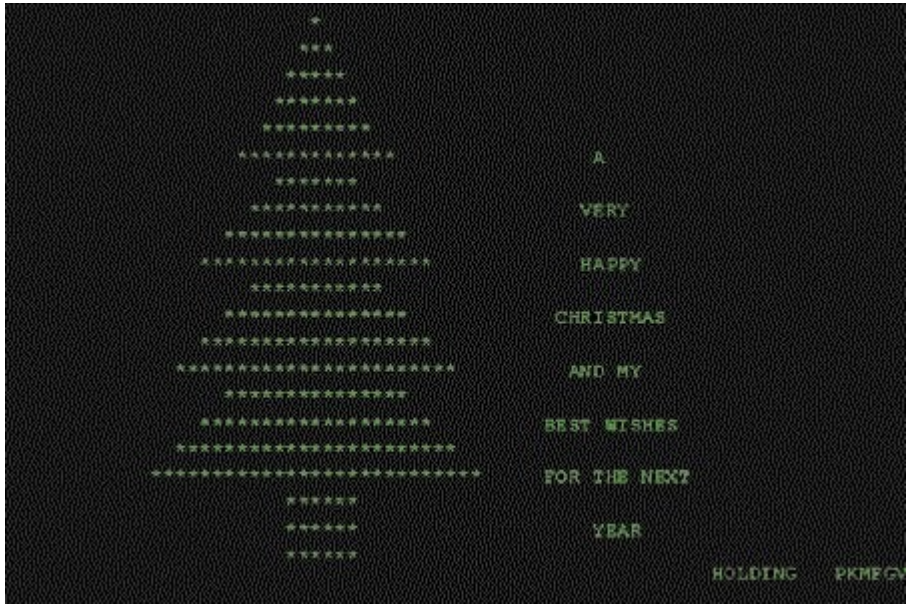
- Jakmile byly výsledky experimentu zveřejněny, administrátoři zakázali další experimenty na jejich systému (UNIX)
- Vedoucí počítačové bezpečnosti nepovolil další experimenty
- Březen 1984 další experiment – virus na Bell – LaPadula systému
- Virus dokázal překročit uživatelské privilegie a pohybovat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

- Raná 80. léta návrat Core Wars (A. K. Dewdney) – programy soutěží o místo v paměti, snaží se zničit konkurenční program
- od roku 1986 pravidelné soutěže
- Software volně ke stažení
- Ukázka: https://www.youtube.com/watch?v=-ytlji6T8R0

Negativizace viru (druhá pol. 80. let)

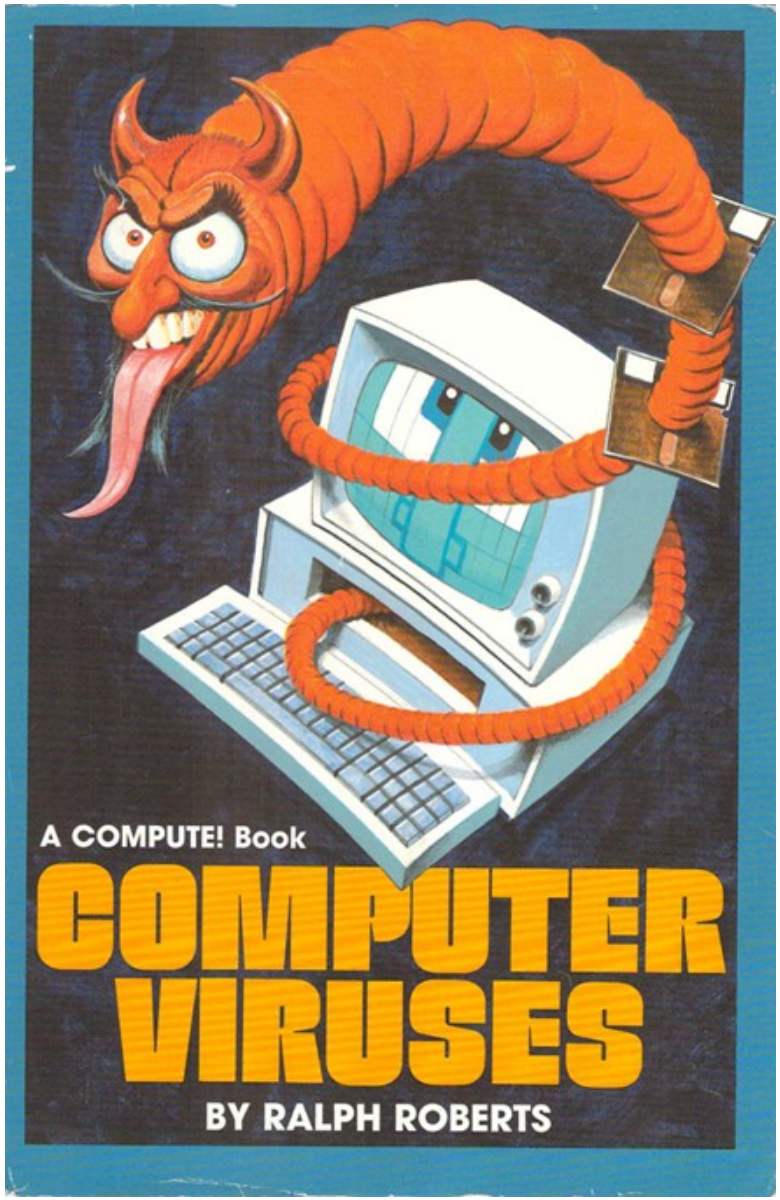
- 1984 - Virus hlavním tématem prezentace Freda Cohena na konferenci o počítačové bezpečnosti
- 1985 - první článek o počítačových virech v magazínu Times
- Brain virus (1986) – první PC virus – infikoval soubory s příponou exe a com
- 1987 - Virus Lehigh – první file infector, který se dostal do širšího povědomí, protože mazal celý disk, ovlivnil antivirovou scénu

- 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
- Nechtěl, aby byl nový obor spojován s počítačovými viry

- Jeruzalem virus – destruktivní náklad, svého vzniku, autor Yisrael Radai, první MS-DOS virus, jež mohl infikovat širokou škálu souborů, vzorem pro další tvůrce virů, různé verze
- Edice - COMPUTE! Book - Computer Viruses – Ralph Roberts - První kniha o ochraně před počítačovým virem – velmi emotivní až hysterické, přichází nový nepřítel, který ohrožuje naše harddisky


A COMPUTE! Book
COMPUTER VIRUSES
BY RALPH ROBERTS

Morris Worm – mediální virus

- Tvůrce student Robert Morris
- Autor původně vůbec nezamýšlel vytvořit nebezpečný program
- 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 – obraz nebezpečných hackerů, debaty s odborníky, antropomorfizace viru

- Morris byl za svůj čin odsouzen ke 400 hodinám veřejných prací
- Počítačový červ také upozornil na zranitelnost internetové sítě a nedostatečné institucionální zázemí pro potírání digitální kriminality
- Vznik institutu CERT (1988), který se specializuje na otázky digitální bezpečnosti.

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

AIDS Trojan (1989)

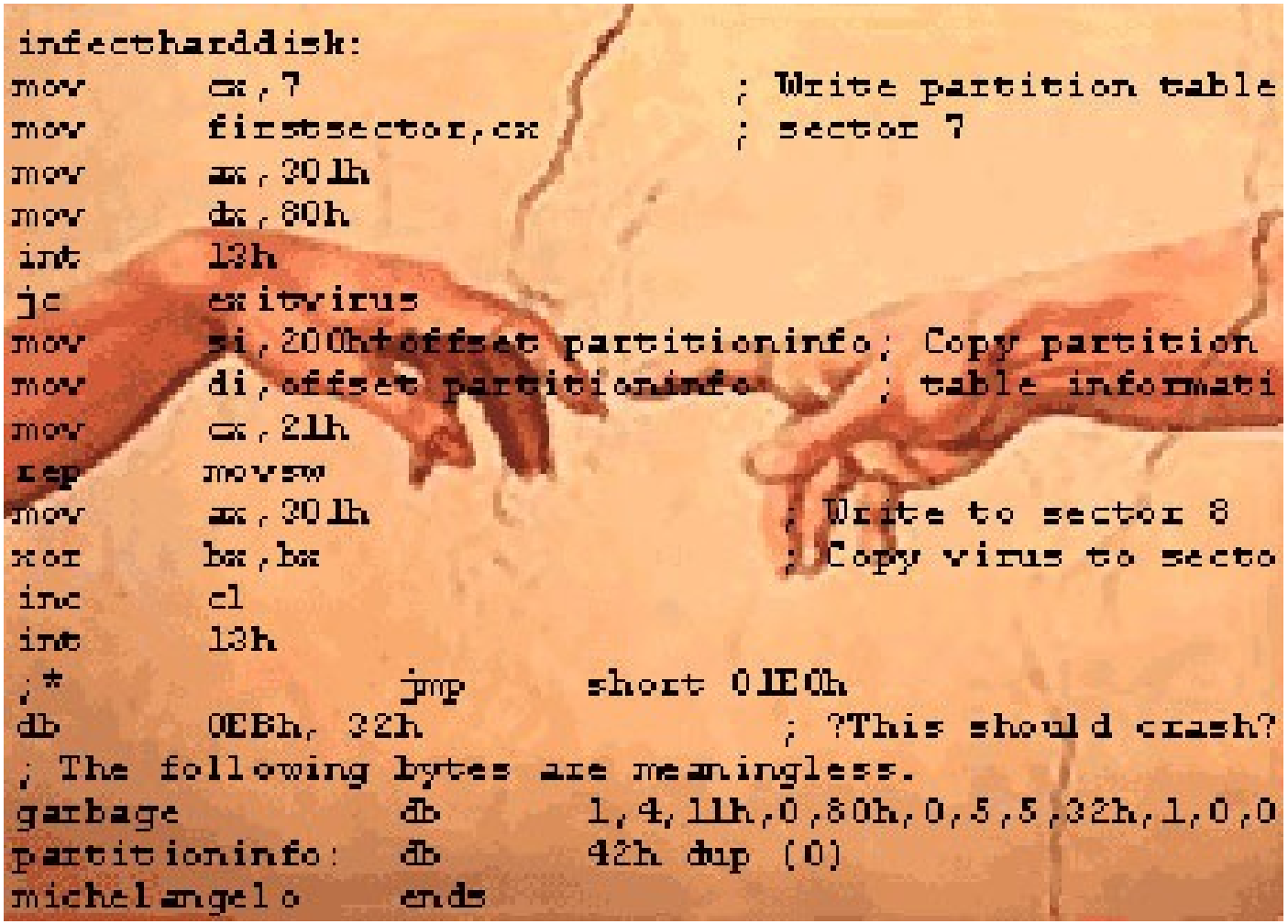
- v roce 1989 odesláno 10 00 kusů disket s informacemi o AIDS
- program se instaloval do složky, ale přitom vytvořil skrytou složku s jiným programem, který po několika spuštěních počítače zašifroval harddisk
- objevila se zpráva, že pokud chce uživatel rozšifrovat data a obdržet šifrovací klíč musí zaplatit poplatek

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

- **Nové viry**
- Polymorfní - při šíření se modifikují
- mnohostranné viry (multipartite virus) - infikují různé oblasti v počítači, soubory i systémové oblasti disku (soubory exe, com nebo boot sektor)
- stealth viry - viry, které se dokáží maskovat v systému – virus Frodo

- obliba virtuálních bulletinů zvaných Virus-exchange boards – komuikační platforma pro tvůrce virů
- Centrem tvorby virů – Bulharsko, Rusko
- 1991- na Virus-exchange boards se objevují konstrukční soupravy, které umožňují vytvoření vlastního viru prakticky komukoliv
- 1992 – Generátory virů - Běžný uživatel si mohl během několika sekund vytvořit vlastní virus.

Michelangelo virus (1992)



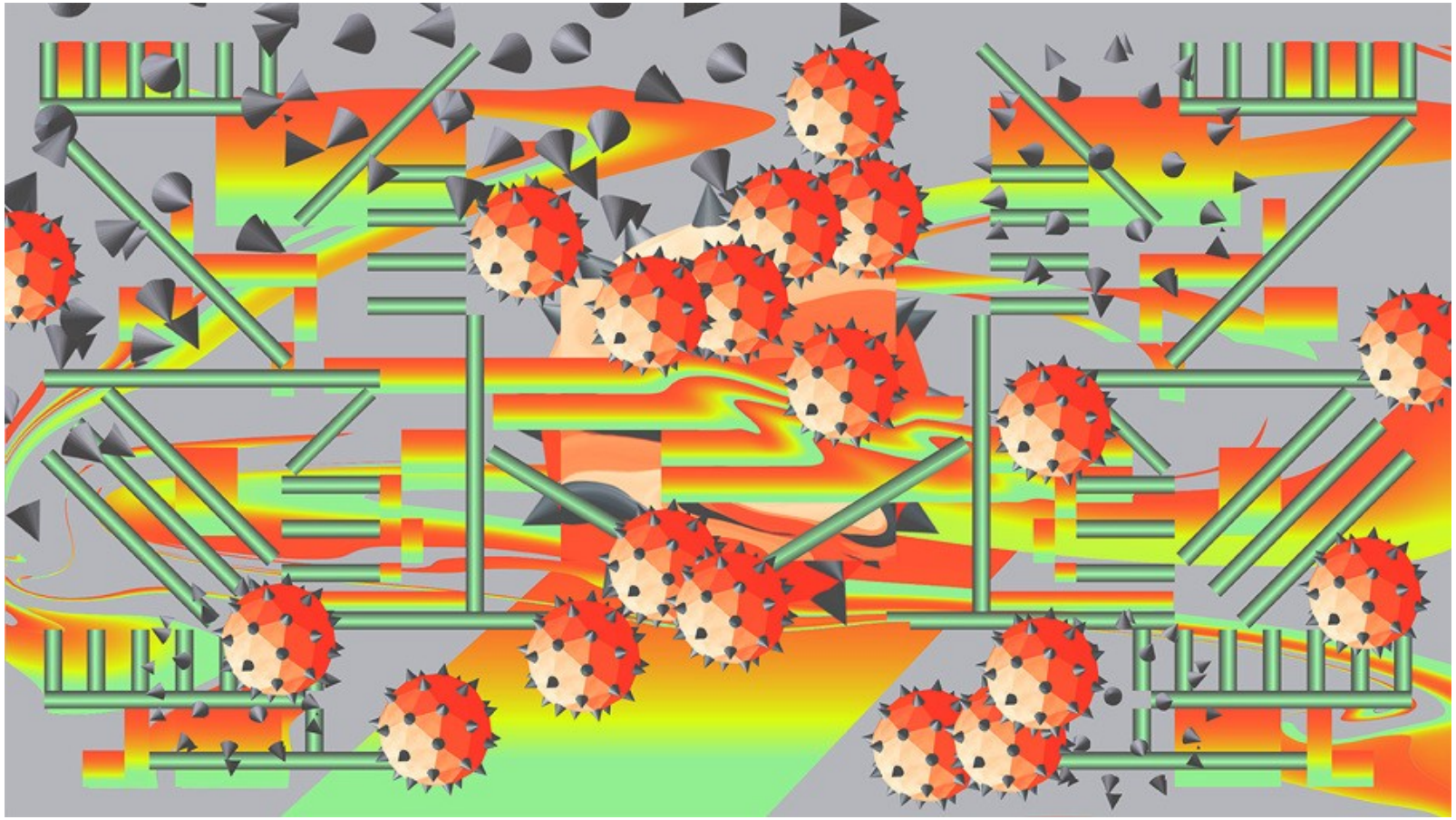
```
infectharddisk:
mov     cx,7                    ; Write partition table
mov     firstsector,cx          ; sector 7
mov     ax,201h
mov     dx,80h
int     13h
jc      exitvirus
mov     si,200h+offset partitioninfo; Copy partition
mov     di,offset partitioninfo     ; table informati
mov     cx,21h
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
```

- Způsobil masovou hysterii
- Přepisoval data na pevném disku
- šířil se prostřednictvím softwaru uloženého na disketách od různých prodejců
- Johnem McAfee předpověděl, že tento virus zasáhne stovky tisíc počítačů
- Prodej antivirových programů se prudce zvýšil
- Reálný dopad byl mnohem menší

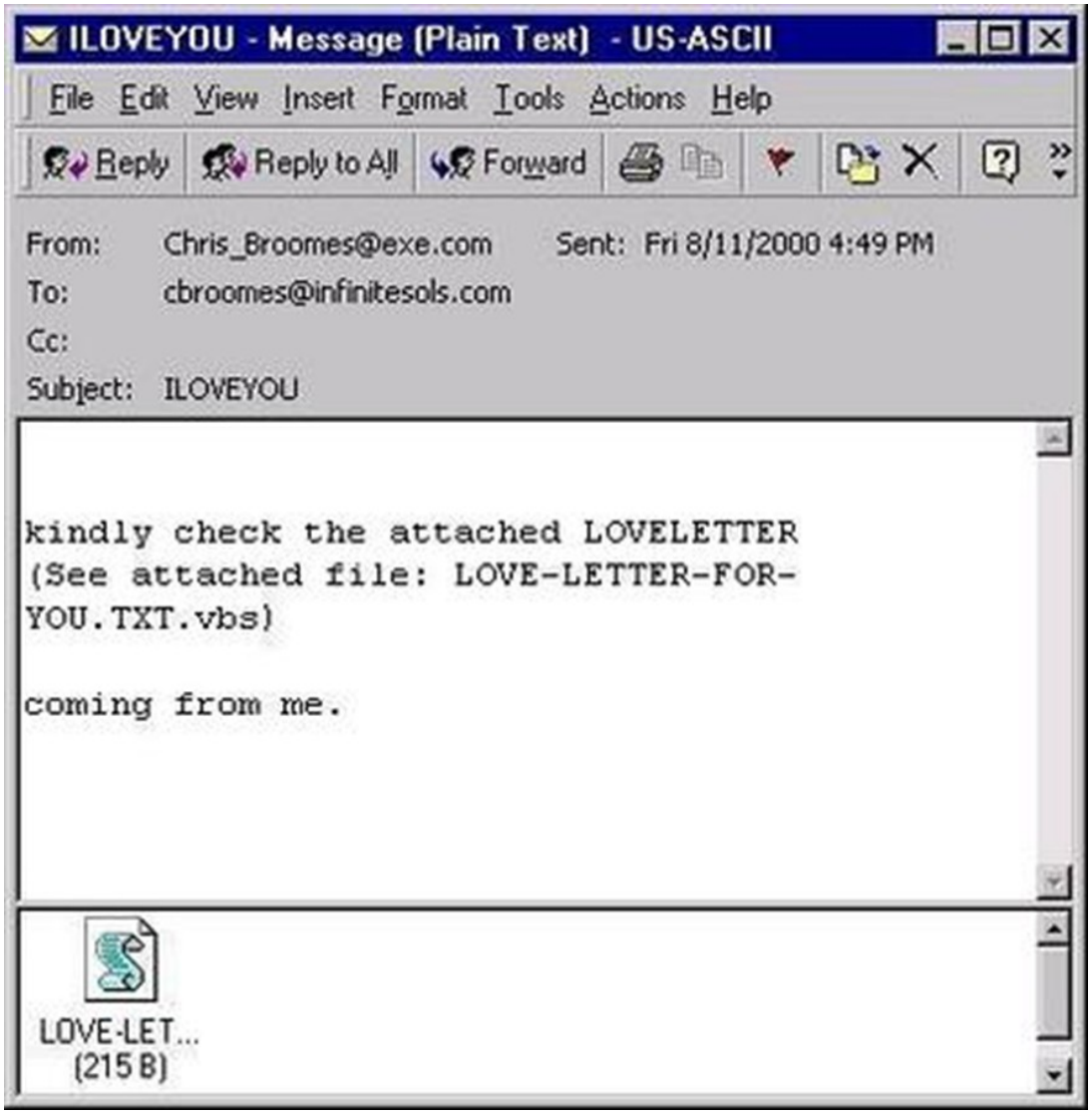
Solar Sunrise (1998)

- Virus, který ovládl zhruba 500 vládních vojenských systémů
- 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)



- Infikoval 10 procent počítačů připojených k internetové síti
- Skrýval se v emailové příloze
- Jakmile byl aktivován rozeslal sám sebe na všechny adresy uložené v emailovém adresáři
- Autoři: Onel de Guzman, Irene de Guzman a Reomel Lamores

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

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

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