C.1 ISTORIA MAȘINILOR ARTIFICIALE ȘI EVOLUȚIA SECURITĂȚII CIBERNETICE

PAUL A. GAGNIUC

Academia Tehnică Militară „Ferdinand I”

PRINCIPALELE PĂRȚI ALE PREZENTĂRII

C.2 Istoria mașinilor artificiale și evoluția securității cibernetice:

- C.1.1 ISTORIA MAȘINILOR ARTIFICIALE DE UZ GENERAL
- C.1.2 EVOLUȚIA ALPICAȚIILOR MALWARE
- C.1.3 EVOLUȚIA SOLUTIILOR DE SECURITATE
- C.1.4 SISTEMELE DE OPERARE ȘI STRATUL DE PORTABILITATE

C.1.1
ISTORIA MAȘINILOR ARTIFICIALE DE UZ GENERAL

Prima placă grafică(I) – semnal digital (1745)

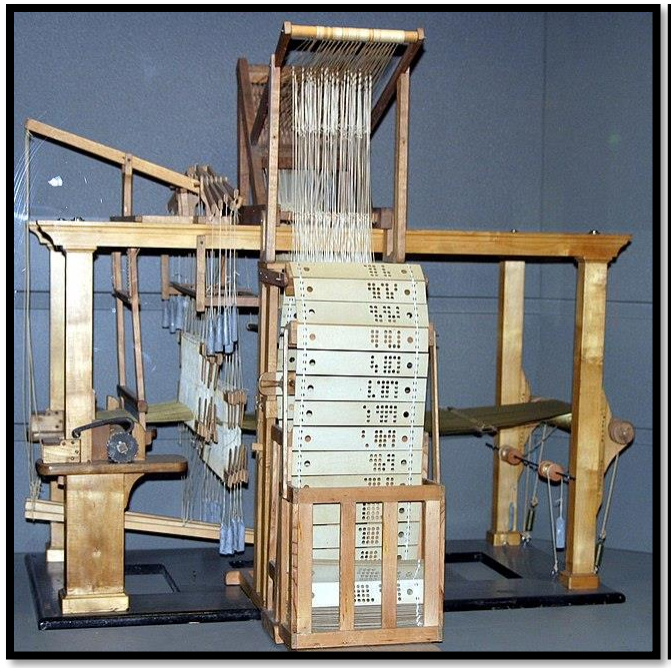
- Prima mașină de țesut cu memorie binară pe carduri!

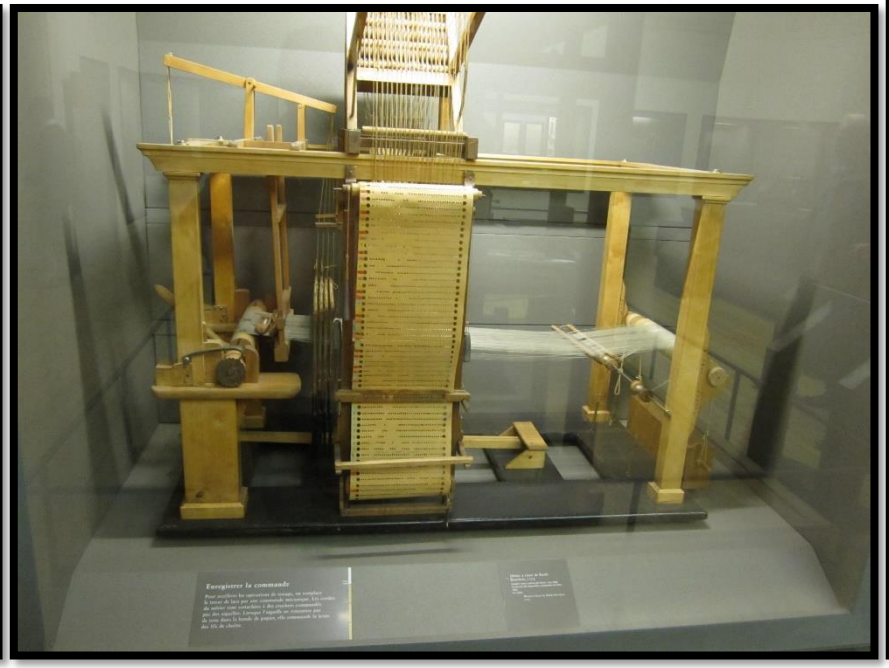
Prima imagine digitala din lume !

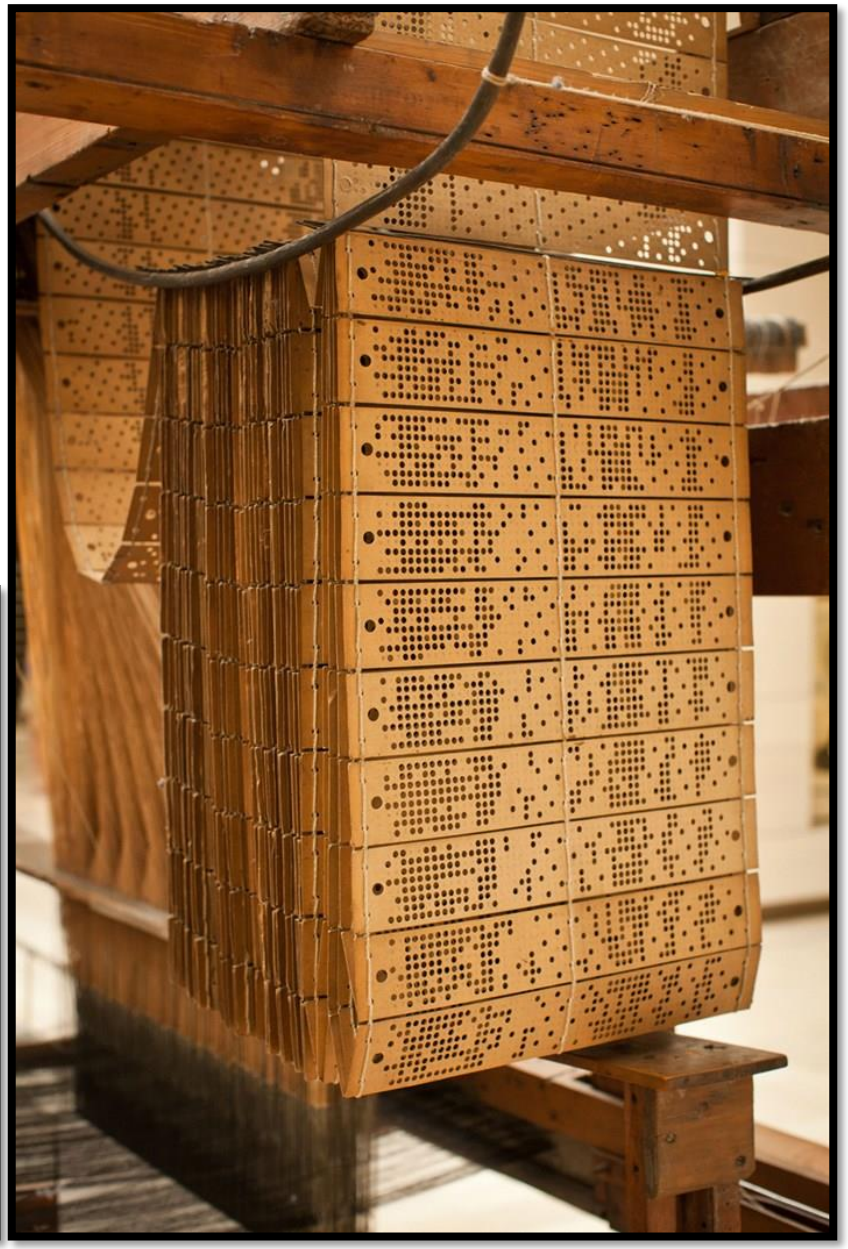
Imaginea este doar un exemplu fictiv!

Prima placă grafică (II) - 1745

- Gaură – 1
- Lipsă – 0







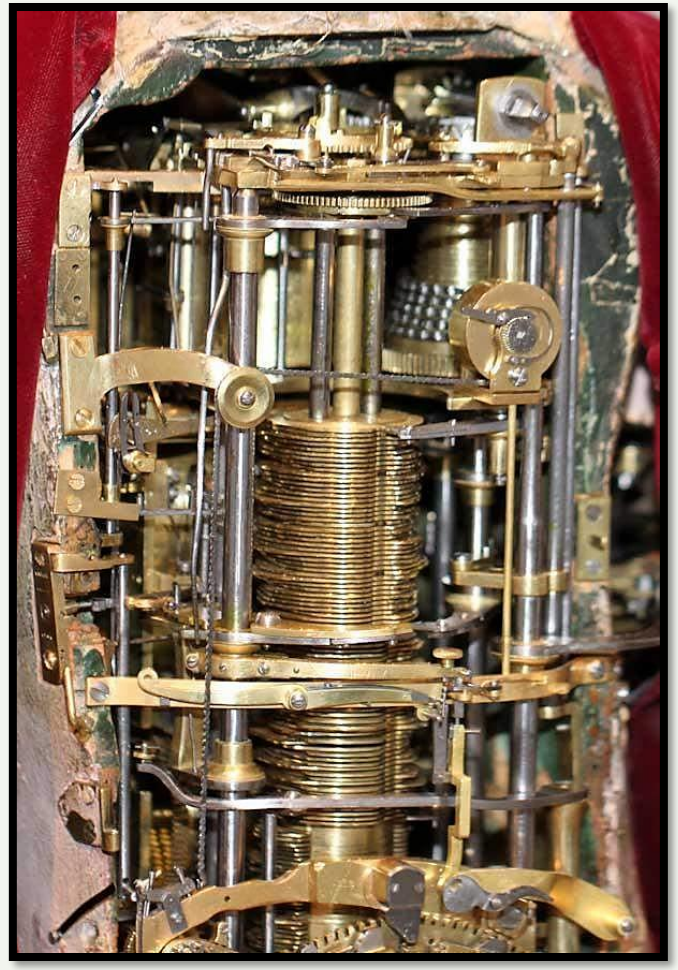
Roboți mecanici cu memorie (roboți - 1774)

The writer (1774)

https://www.youtube.com/watch?v=yYta1Y_hEJI

Roboți mecanici cu memorie (roboți - 1774)

- Semnal analog.
- 30-40 de caractere.
- memorie – ax cu discuri ale căror proeminențe împing un braț mecanic.
- Parțial asemănător cu cilindrul unei cutii muzicale.



Semnal digital

Calculatoare mecanice (uz general)

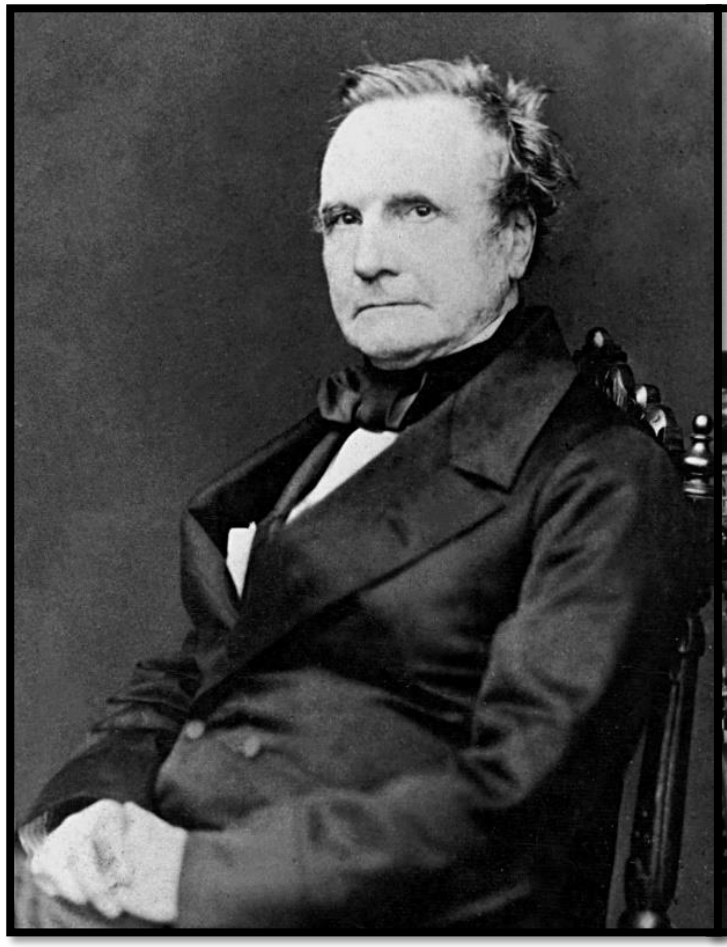
Sfarsitul revolutiei industriale

Charles Babbage; "Motorul Analitic" 1830

Dupa 106 de ani

Konrad Zuse; Z1 1936

Calculatorul theoretic "Motorul Analitic" - 1830



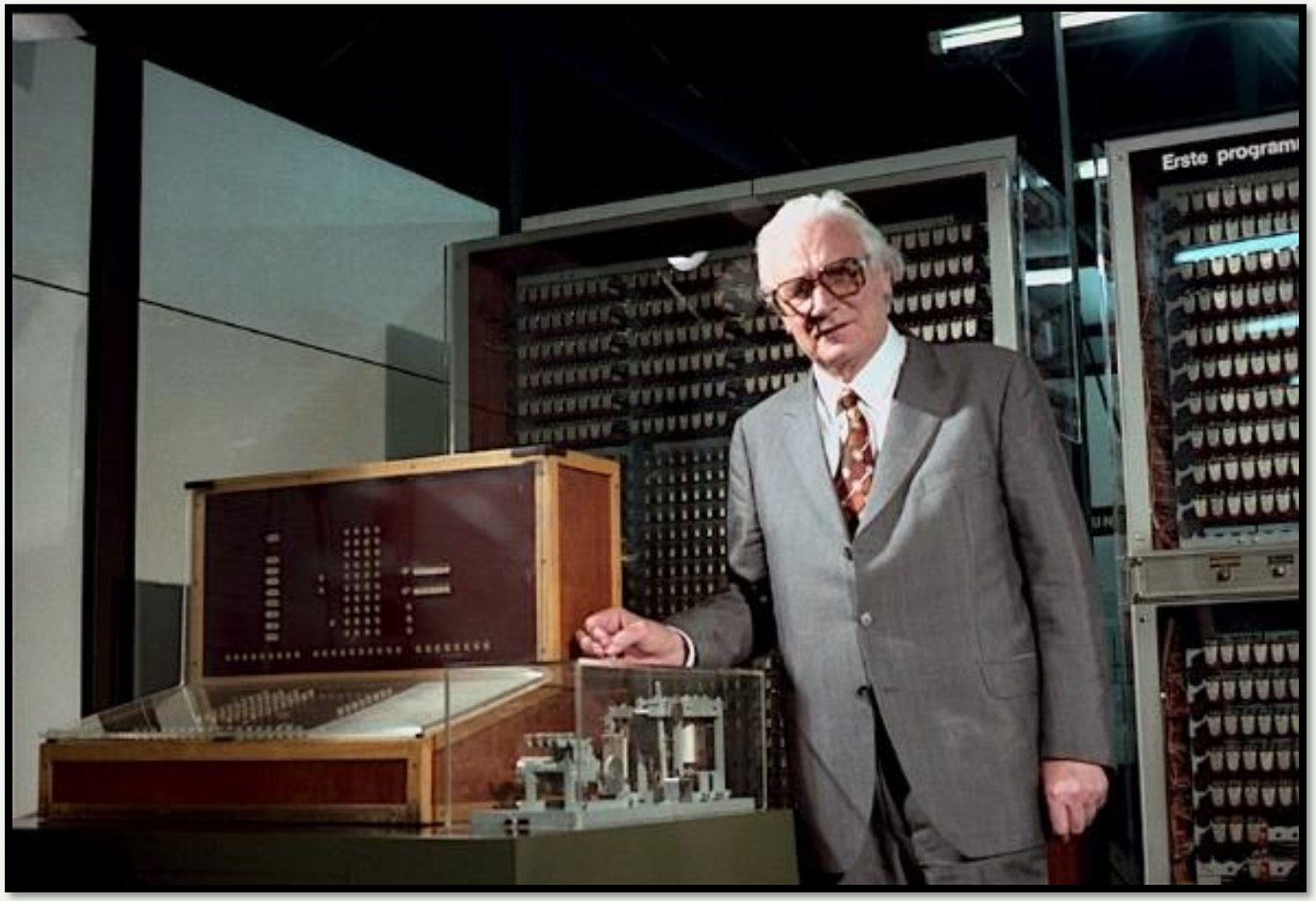
Charles Babbage (hardware)
Ada Byron (programmer)

Calculatorul Z1 -1936

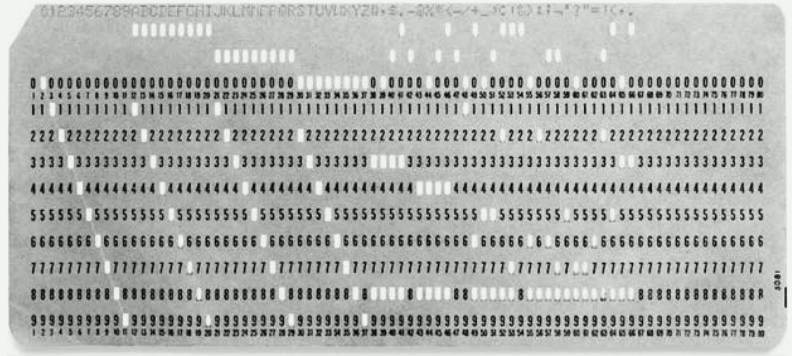
Konrad Zuse

Calculatoare electro-mecanice

Calculatorul Z3 -1941; 5 ani mai târziu…



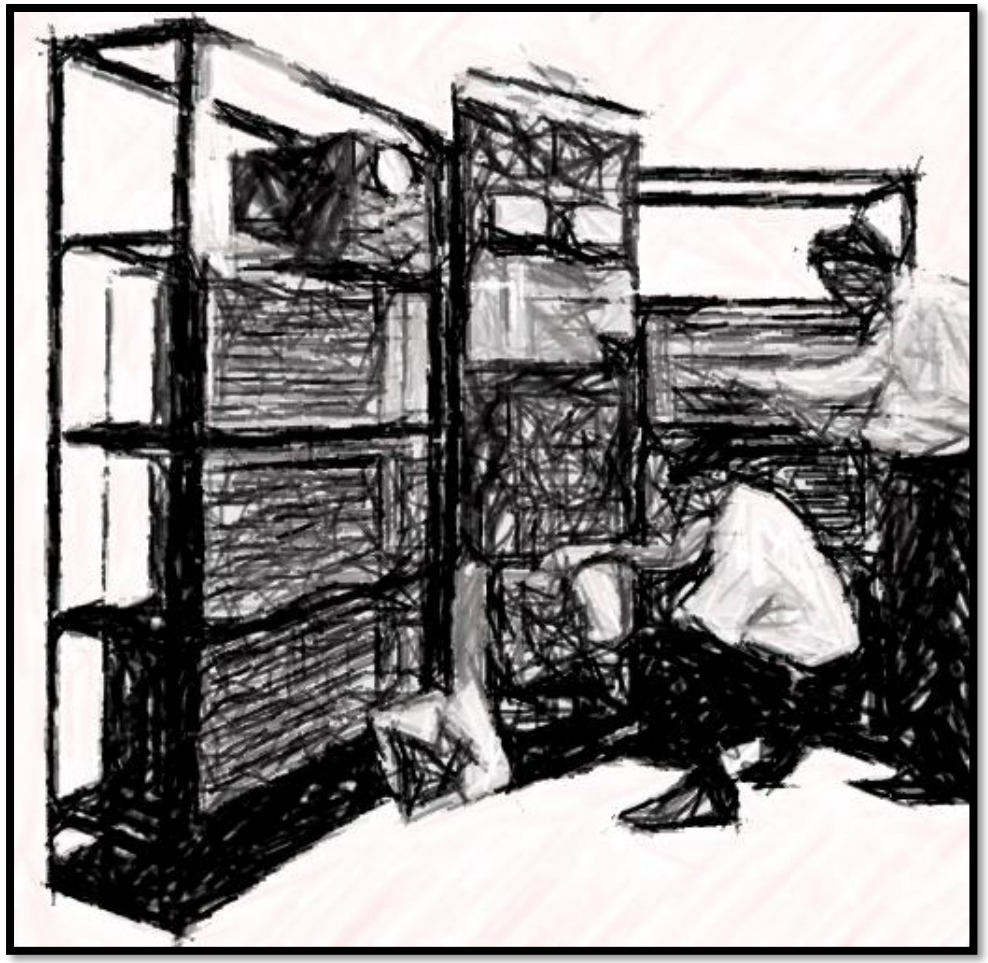
Konrad Zuse



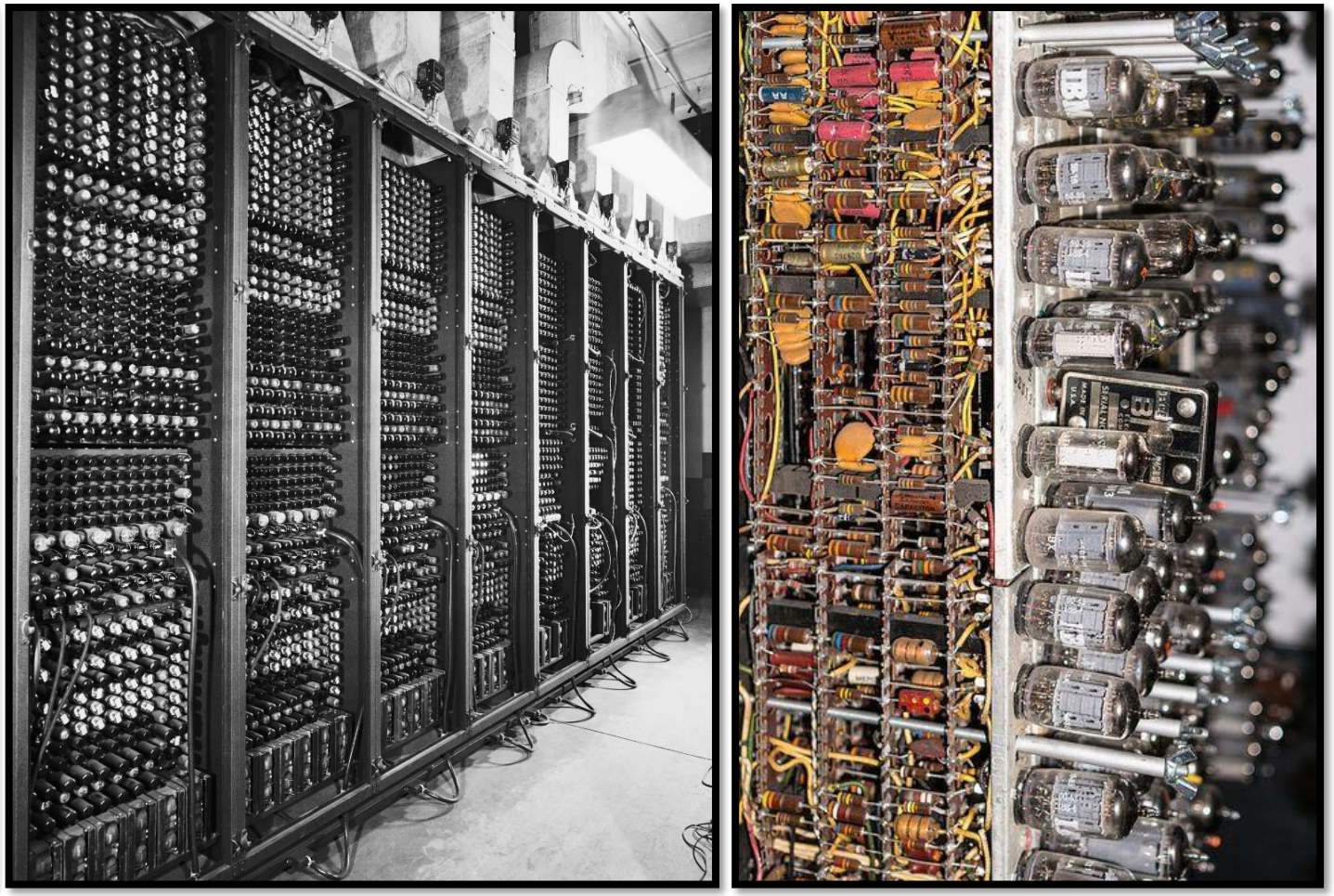
Releu electro-mecanic

Calculatoare electronice

TRADIC – 1950 (pe 800 tranzistoare) ⟵ ENIAC – 1945 (pe 17k lampi)



(Transistorized Airborne Digital Computer)



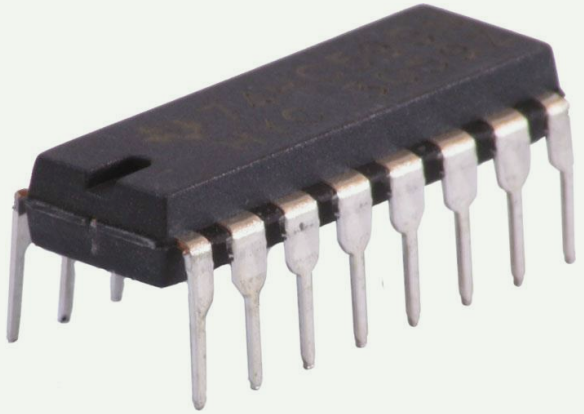
(Electronic Numerical Integrator and Computer)

Calculatoare electronice (piese discrete)

Releul
1835

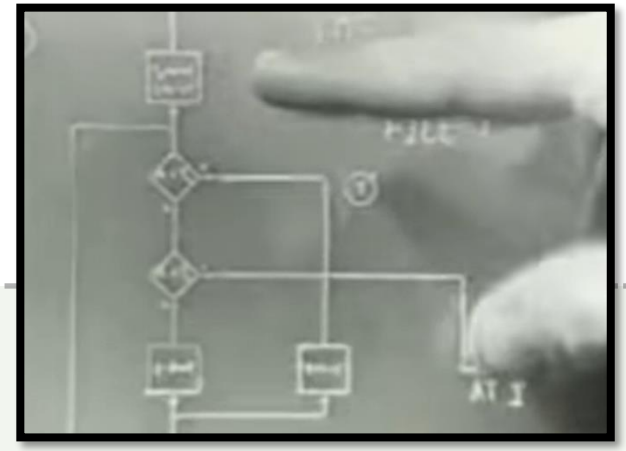
Tuburi vidate
1907

Tranzistori
1947

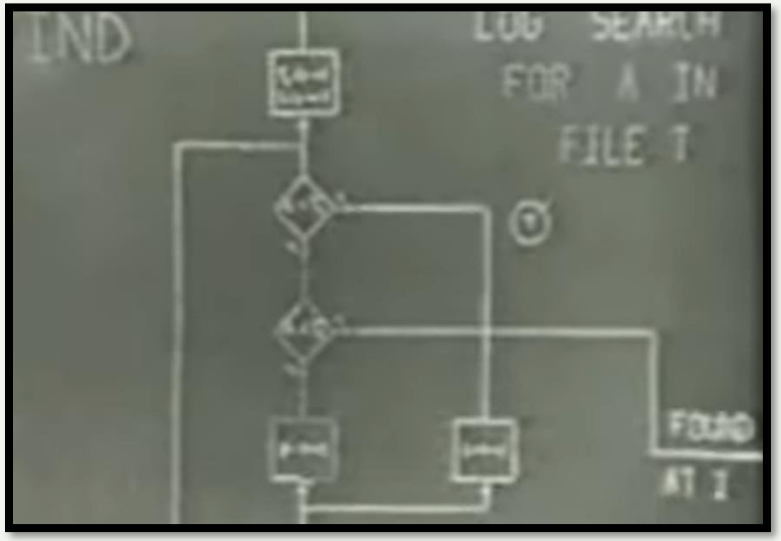


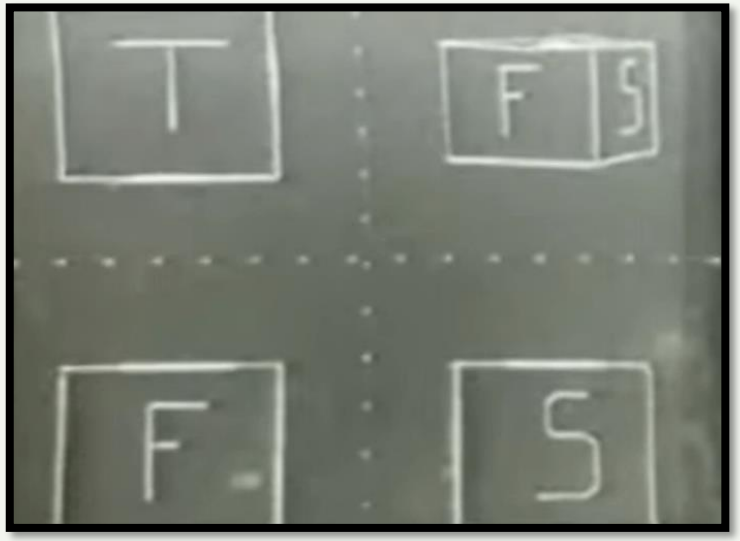
Circuit Integrat
1963

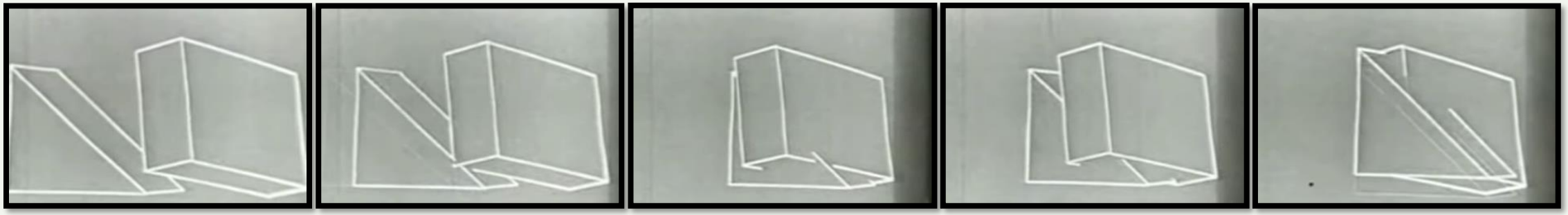
Prima interfata grafica (GUI)



- 1962 (diagrame, obiecte 3D …)





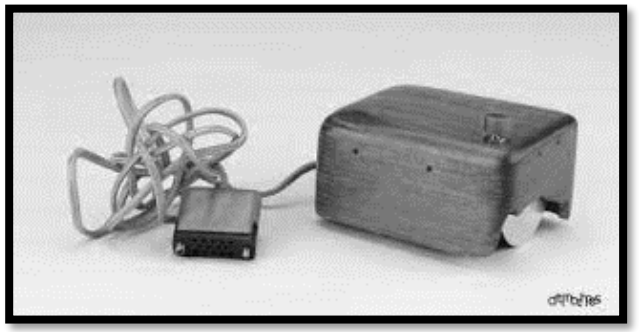


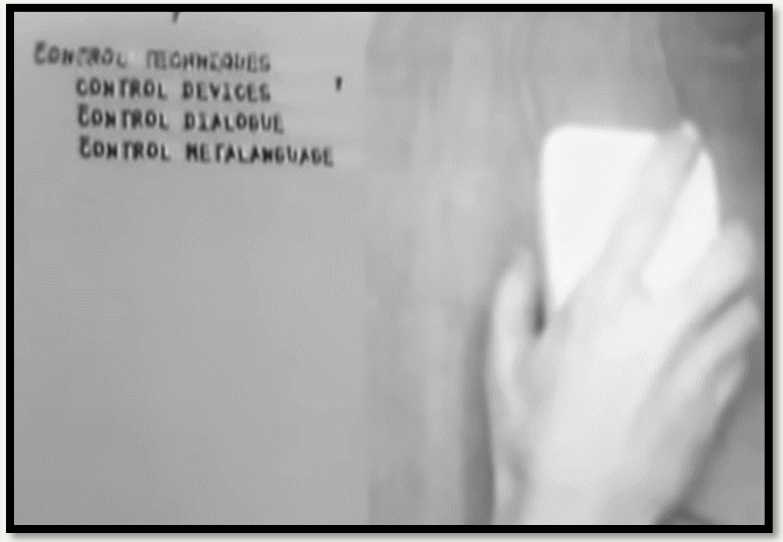
940 SDS

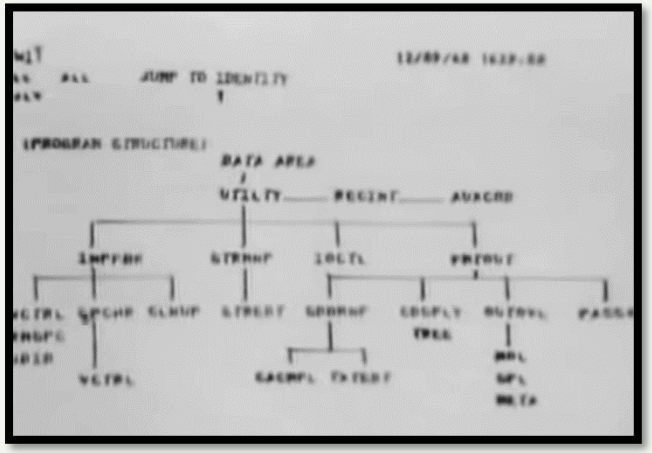
1968

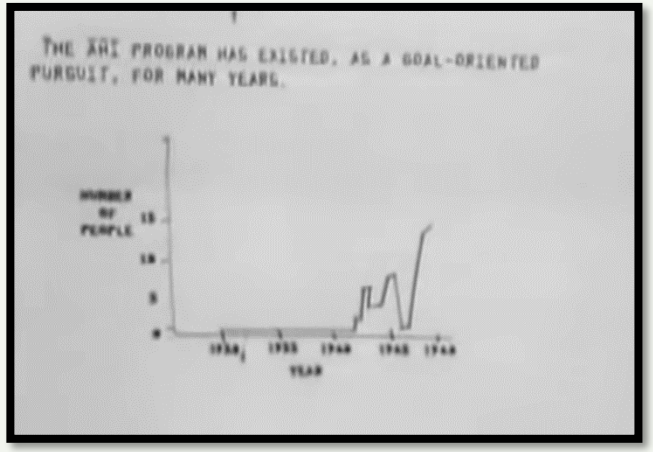
- *Douglas Engelbart* a inclus conceptul de hipertext, care este un element de bază al HTML și al World Wide Web.
- Augmentarea (îmbunătățirea în latină) a interacțiunii om-mașină.

Douglas Engelbart - Decembrie 9, 1968:
Mother of all demos









ASCII

Line Feed (LF:10)

Carriage Return (CR:13)

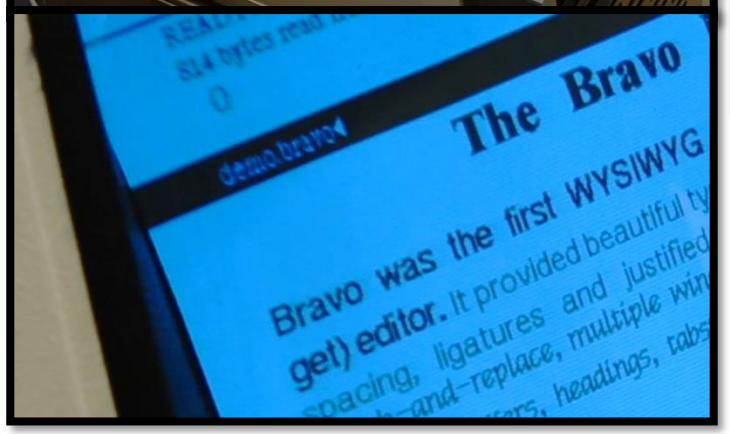
American Standard Code for Information Interchange – (128 caractere; versiunea extinsa 255 caractere)

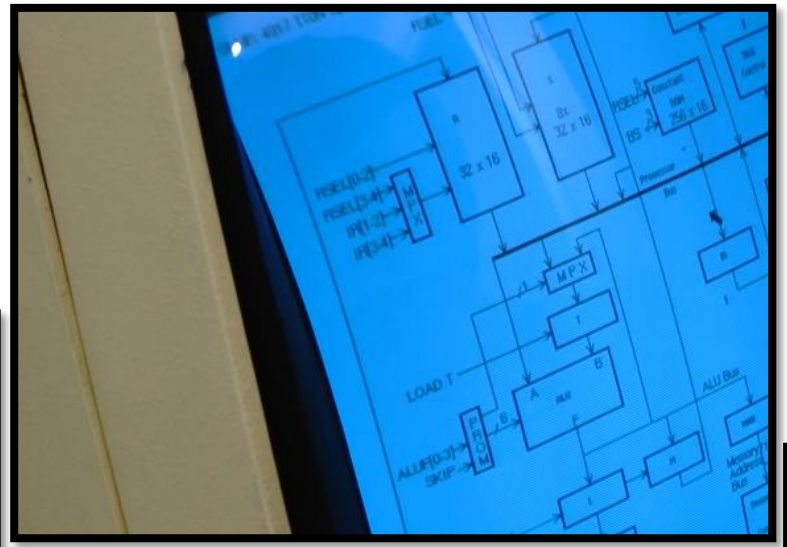
Poziția tastelor pe tastaturile moderne?

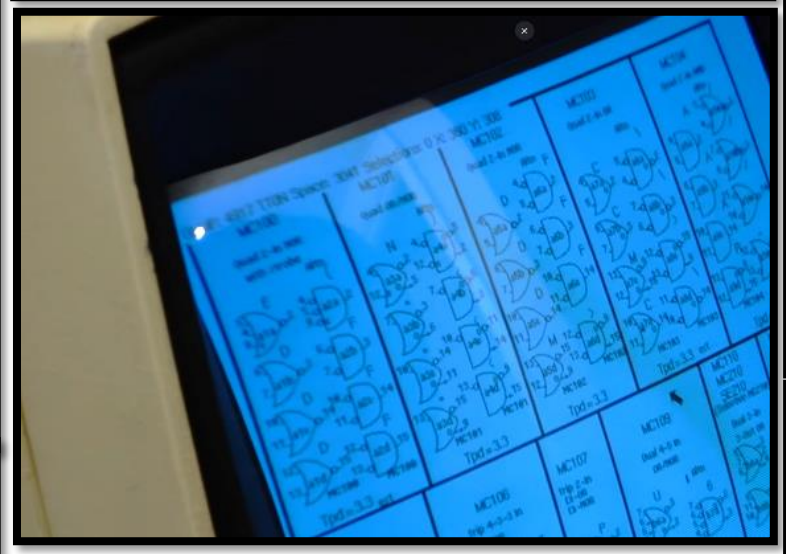
Ce reprezintă ASCII?

Xerox Alto

1973



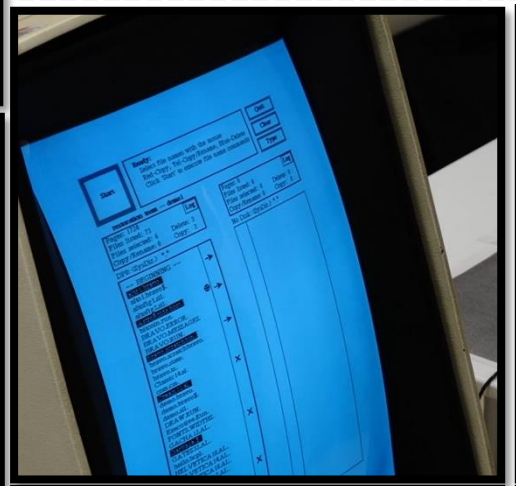


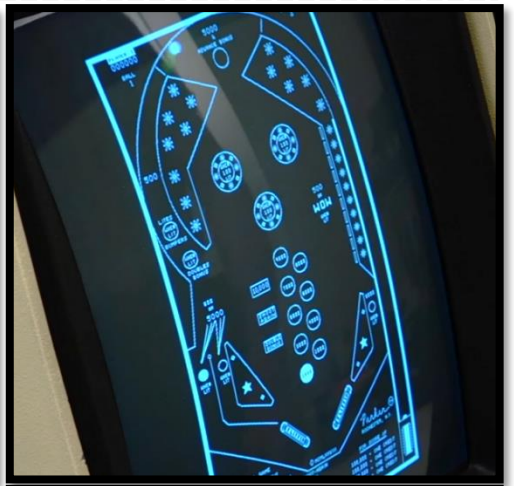


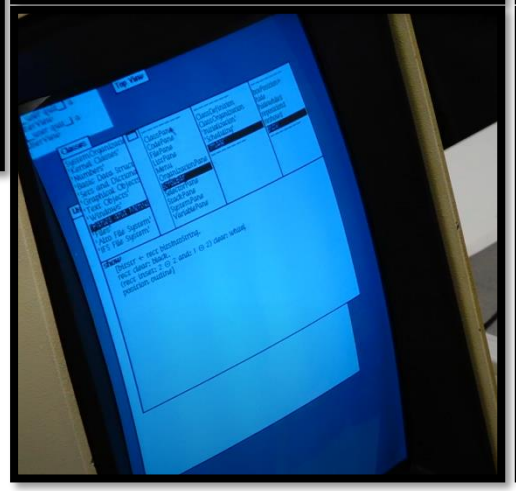
Software modern

Alto Operating System (AOS)

Sursa tuturor desktop-urilor !

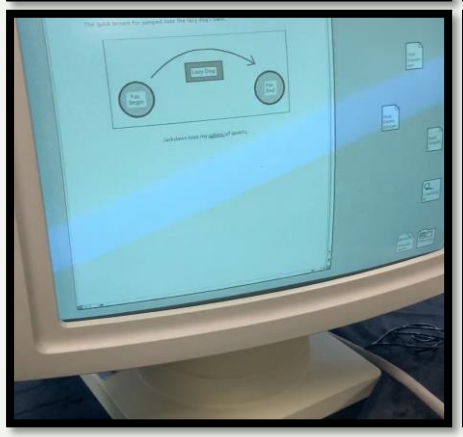






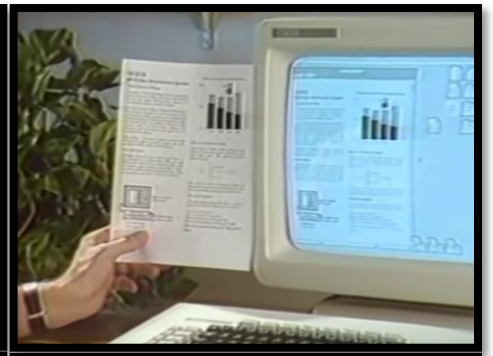
Xerox Star 8010 Computer

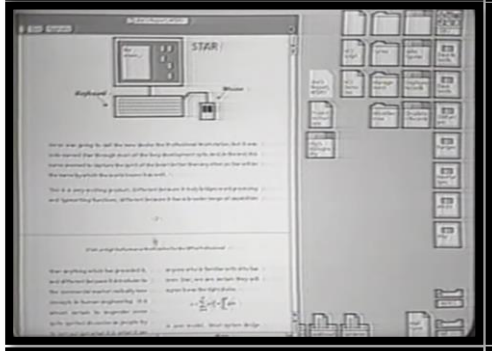
1981

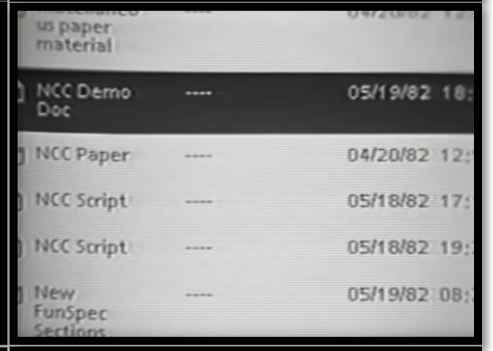


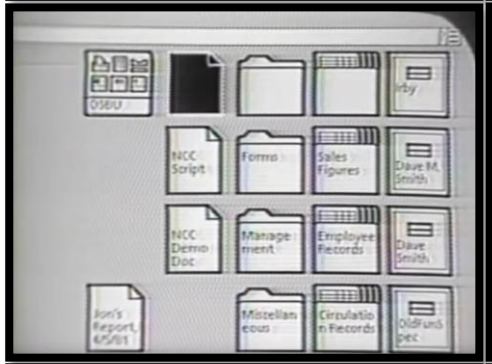
Xerox Star OS
16-bit
8Mhz

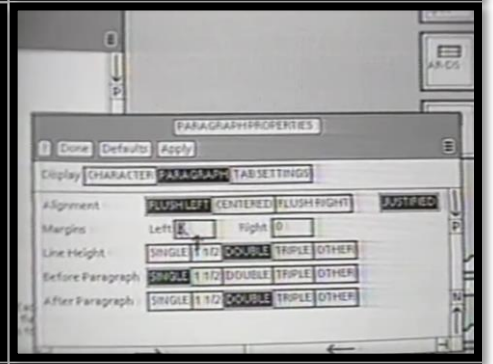
Ce observam?

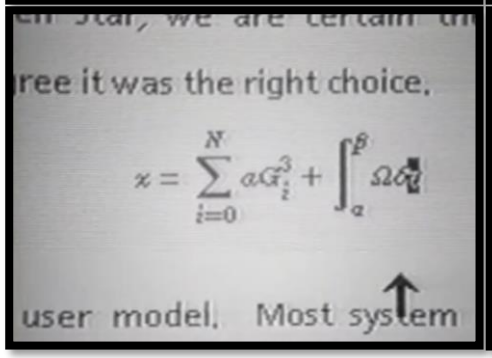


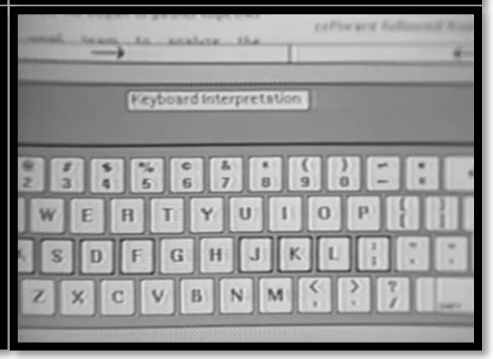




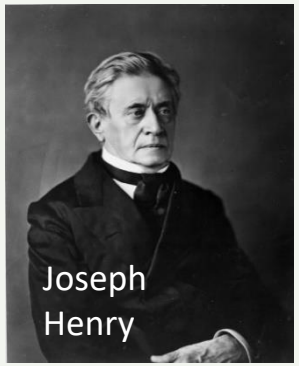


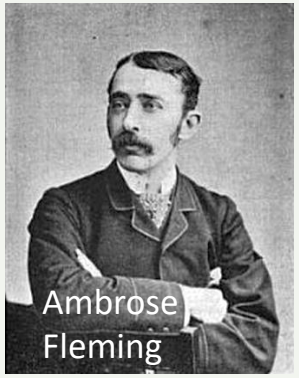


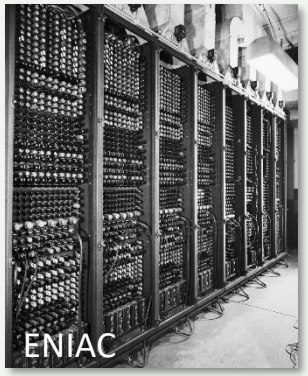


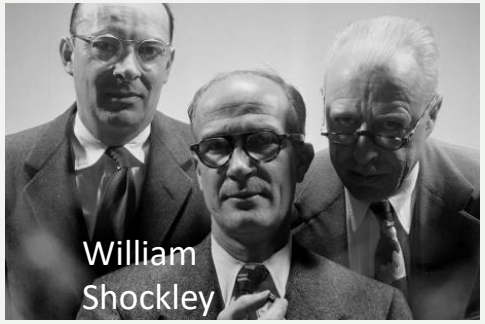


Recapitulare ! De la releu la tranzistor !





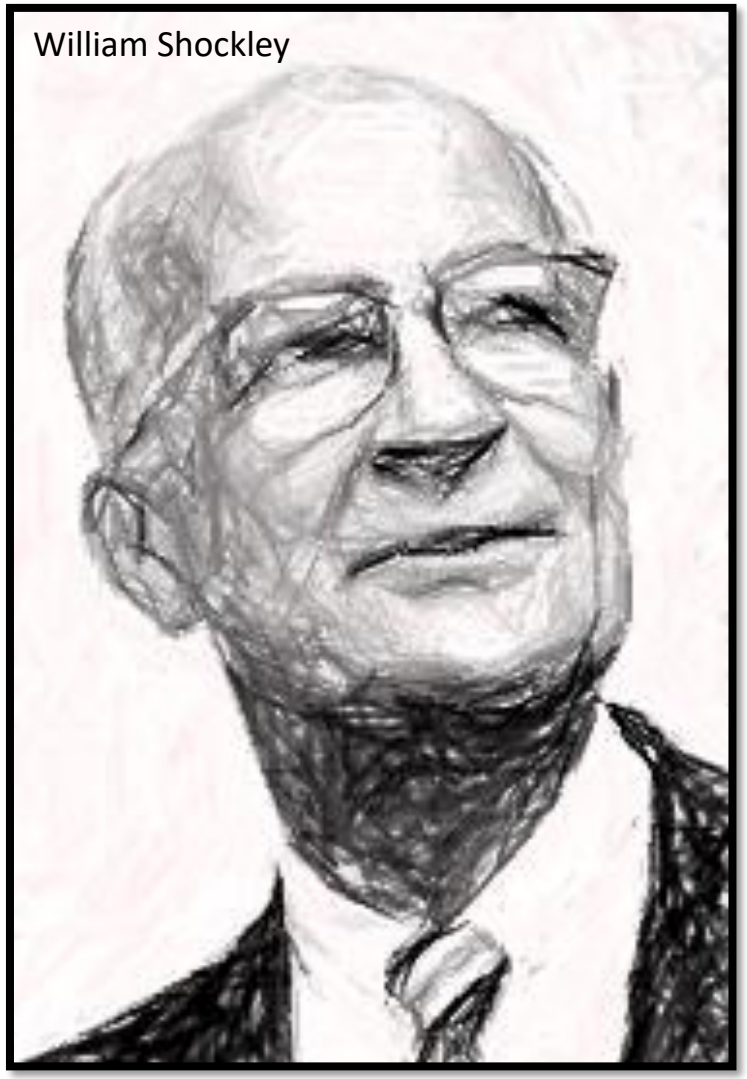


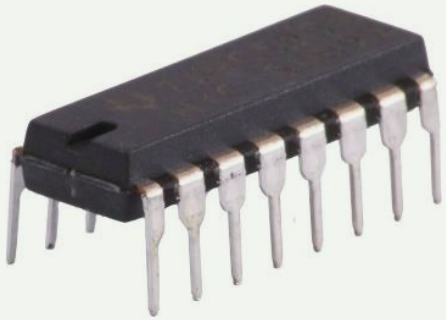


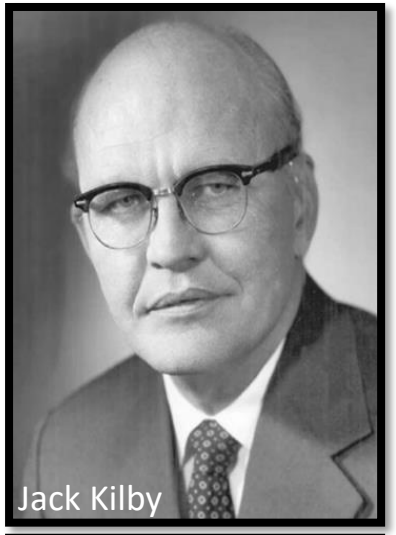
- Releu
- Lămpi
- Tranzistoare
- CI (Circuite Integrate)

Recapitulare ! Era semiconductorilor !

Descoperirea efectului de tranzistor → Compactarea in Circuite Integrate (CI) → Primele calculatoare desktop







C.1.2
EVOLUȚIA APLICAȚIILOR MALWARE

Cand apar primele aplicatii malware?

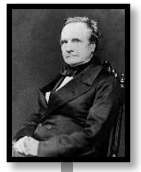
Phone

Calculatoare personale (PC)

(1953) Mainframes (calculator central de mare putere)

Rev. Industriala | Calculatoare mecanice si elecro-mecanice | Calculatoare electronice

1830 Babbage



1840

1873

1935
Codul Morse (1837)
si telegraful (1844)

1907

1936 Konrad Zuse z1

1941 Konrad Zuse z3

1945 ENIAC

1947

1954 TRADIC

1963 ASCII

American Standard Code for Information Interchange – 128 chr

1963 Primul GUI

1968 Douglas Engelbart 940 SDS

1972 Xerox Alto

1981 Xerox Star

1987 First Antivirus

Astăzi

99% din toate fenomenele fizice au fost descoperite

WWI (1914-1918)

WWII (1939-1944)

Apariția treptată a aplicațiilor malware din 1971

Explorarea evoluției malware-ului (I)

1970 - 1990

1972

1981

Xerox Alto

Xerox Star

1971 Creeper

*Worm; TENEX OS; ARPANET

1975 Animal

*Trojan; UNIVAC 1100 OS

Mainframe

1982 Elk Cloner

*Boot Virus; Apple II OS

1986 Brain

*Resident Boot Virus; MS-DOS

1987 Stoned

Boot Virus; MS-DOS

1988 Morris

Worm; UNIX; *(resident RAM)

*File Virus; MS-DOS;

Cascade 1987

.exe (resident)

Vienna 1987

.com (non-resident)

*Backdoor; VAX/VMS OS;

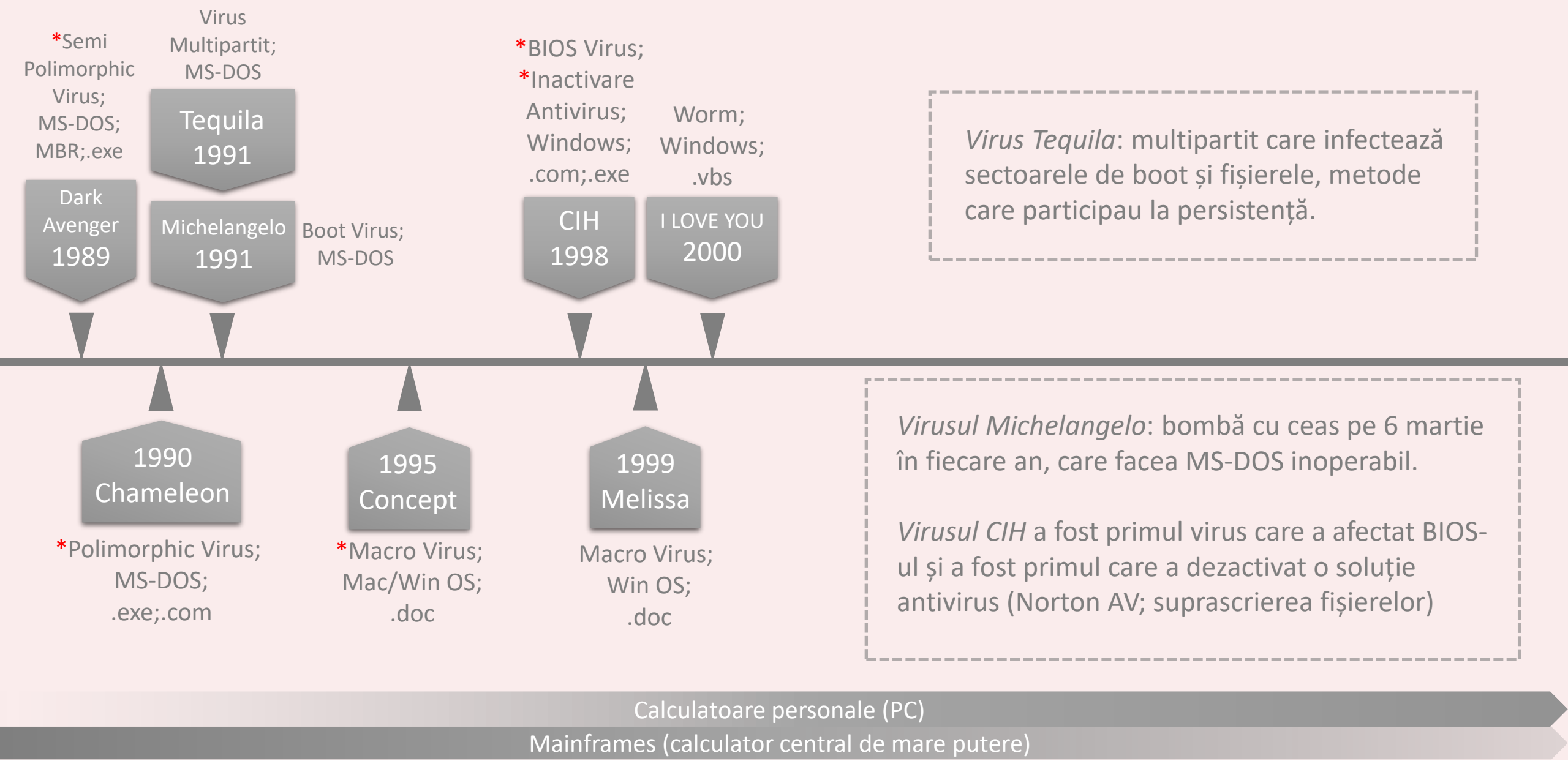
WANK 1989

Virusul Elk Cloner: Un poem era afisat la fiecare 50 de infectari.

Viermele Creeper: Când se autocopia într-un sistem nou, viermele își ștergea fișierul din vechiul sistem de operare. După infectare, afișa mesajul „Sunt Creeper, prinde-mă dacă poți!”

Calculatoare personale (PC)

Mainframes (calculator central de mare putere)



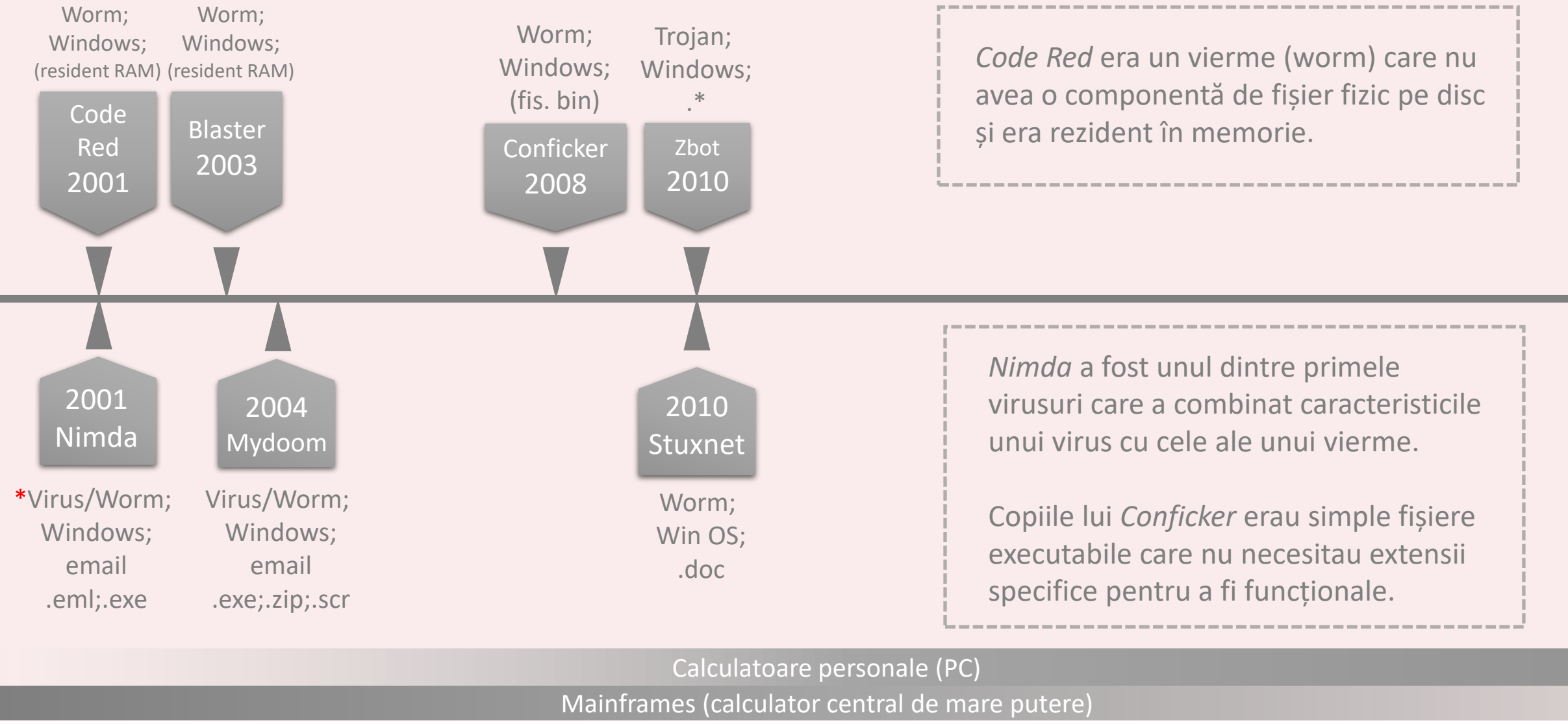
Virus Tequila: multipartit care infectează sectoarele de boot și fișierele, metode care participau la persistență.

Virusul Michelangelo: bombă cu ceas pe 6 martie în fiecare an, care facea MS-DOS inoperabil.

Virusul CIH a fost primul virus care a afectat BIOS-ul și a fost primul care a dezactivat o soluție antivirus (Norton AV; suprascrierea fișierelor)

Explorarea evoluției malware-ului (II)

1990 - 2000



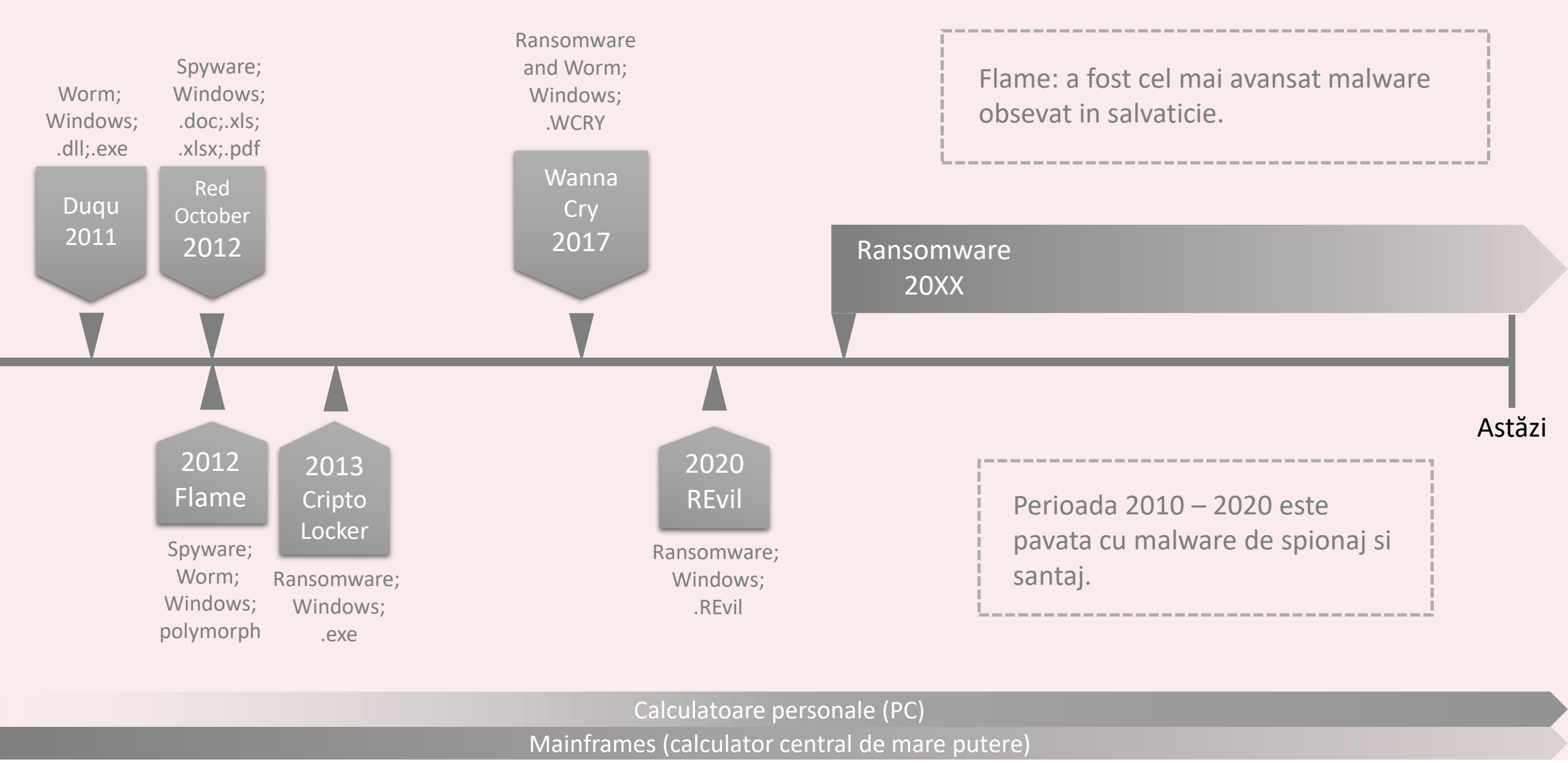
Code Red era un vierme (worm) care nu avea o componentă de fișier fizic pe disc și era rezident în memorie.

Nimda a fost unul dintre primele virusuri care a combinat caracteristicile unui virus cu cele ale unui vierme.

Copiile lui *Conficker* erau simple fișiere executabile care nu necesitau extensii specifice pentru a fi funcționale.

Explorarea evoluției malware-ului (III)

2000 - 2010



Explorarea evoluției malware-ului (VI)

2010 - 2020

Tipuri de malware/Decada

Distributia aproximativa:

Anii 1970

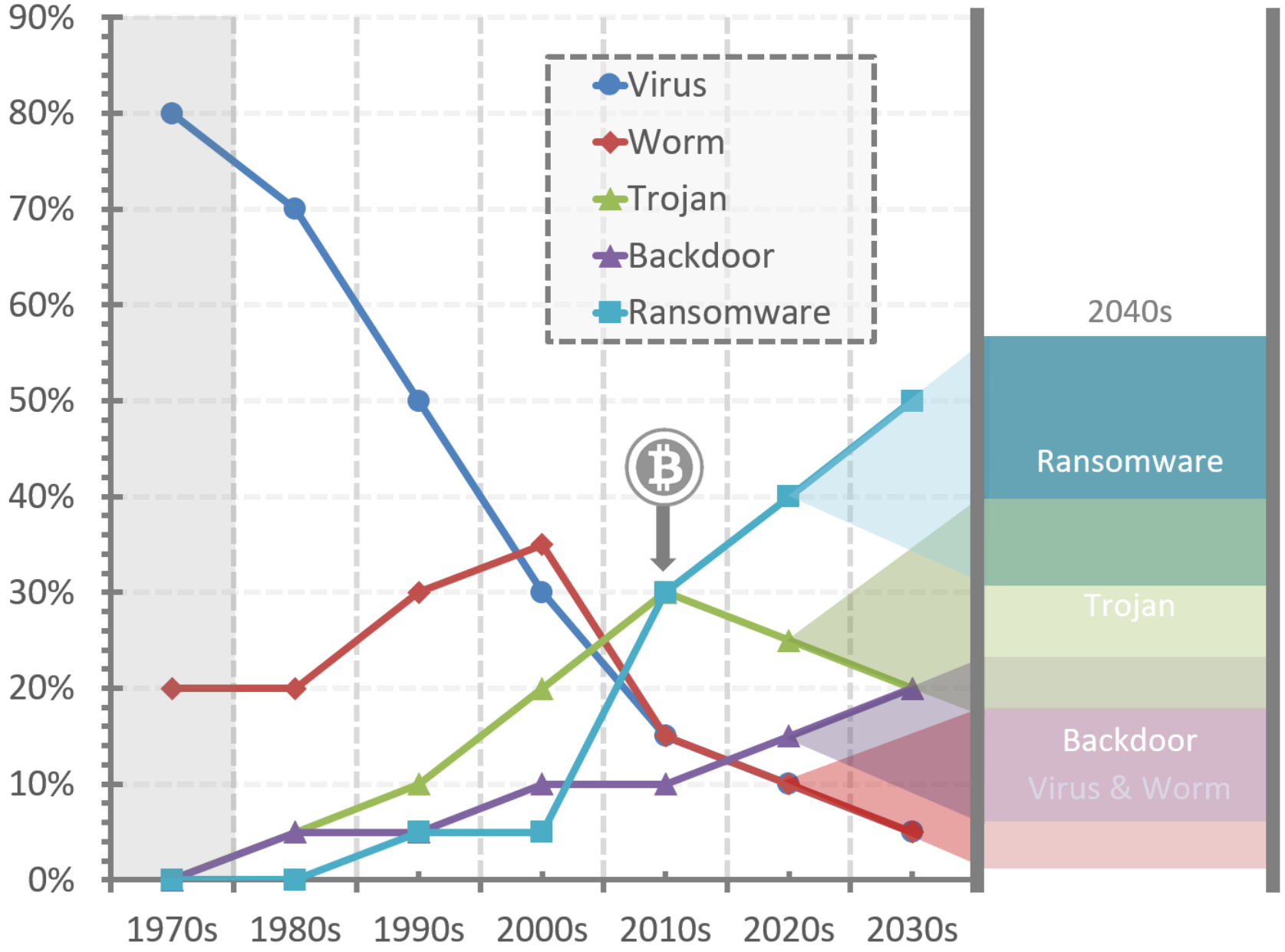
Virus: 80%
(Discuții mai mult teoretice și dezvoltări timpurii)

Worm: 20%
(Apariția primelor viermi, cum ar fi *Creeper*)

Trojan: 0%
(Nu a fost semnificativ recunoscut în acea perioadă)

Backdoor: 0%
(Instanțe limitate)

Ransomware: 0%
(Nu a fost încă dezvoltat)



Tipuri de malware/Decada

Distributia aproximativa:

Anii 1980

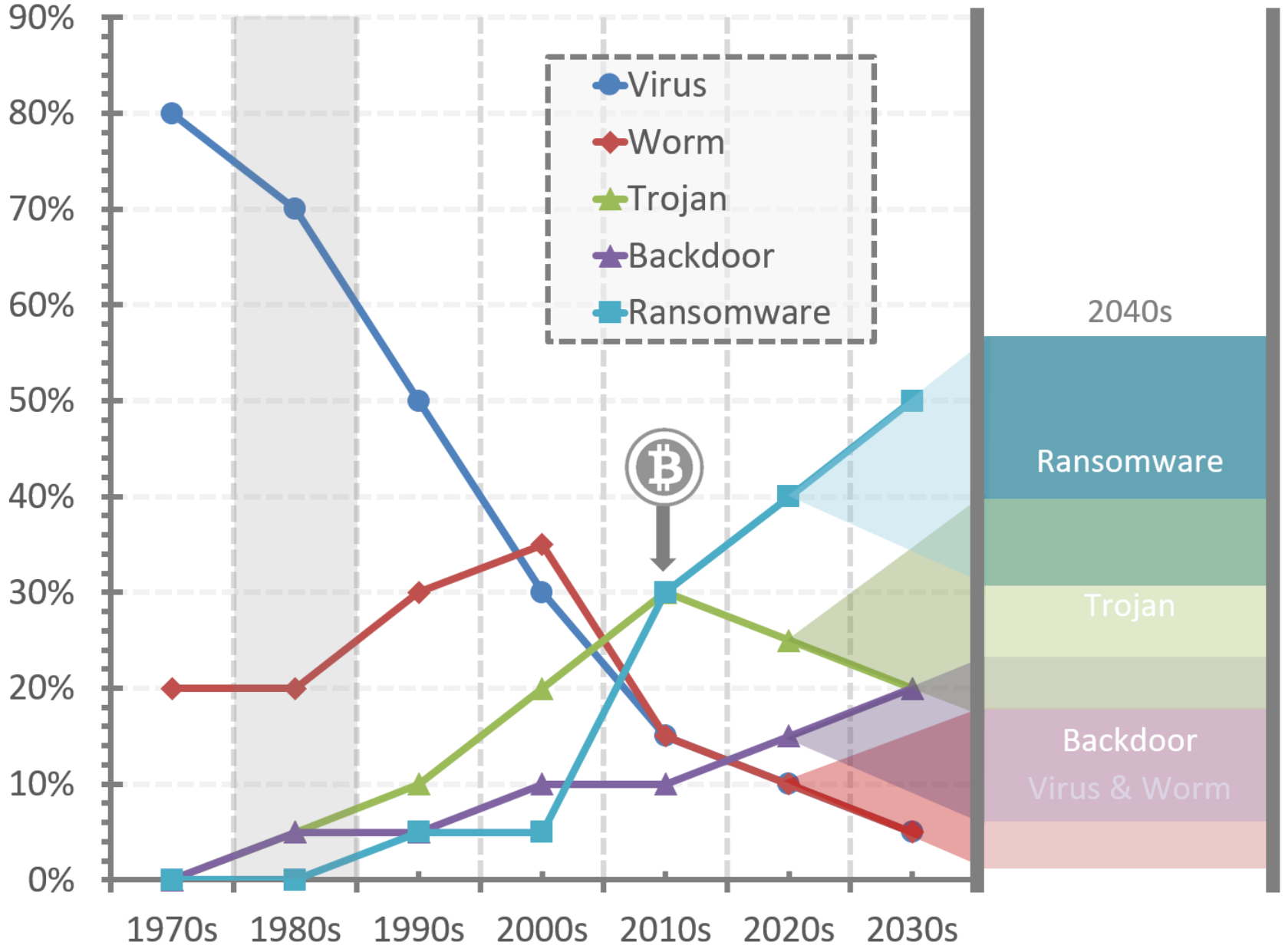
Virus: 70%
(Creșterea virusilor de PC)

Worm: 20%
(Instanțe notabile
precum *Morris Worm*)

Trojan: 5%
(În stadiu incipient,
dar nu proeminent)

Backdoor: 5%
(Începuturile dezvoltării)

Ransomware: 0%
(Nu a reprezentat încă
o amenințare semnificativă)



Tipuri de malware/Decada

Distributia aproximativa:

Anii 1990

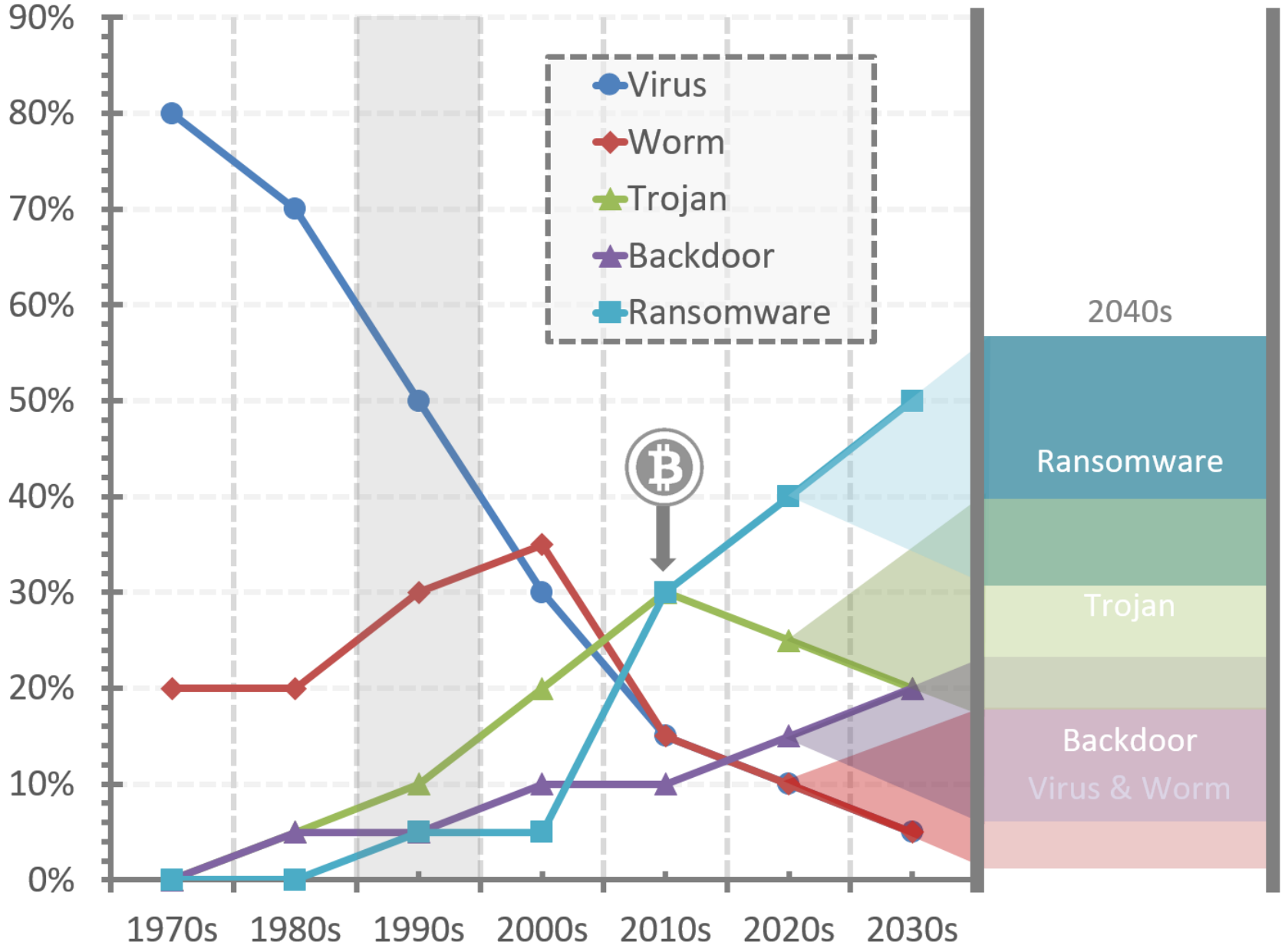
Virus: 50%
(Proliferare larg răspândită)

Worm: 30%
(Activitate crescută,
în special spre sfârșitul anilor '90)

Trojan: 10%
(Începe să câștige teren)

Backdoor: 5%
(Văzut în atacuri mai sofisticate)

Ransomware: 5%
(Formele timpurii încep să apară)



Tipuri de malware/Decada

Distributia aproximativa:

Conturi bancare - identitate reală:
- Cumpărare produse – la adresa – vanzare ulterioara.
- Cont bancar real - persoana frontala – ridicare bani.

Anii 2000

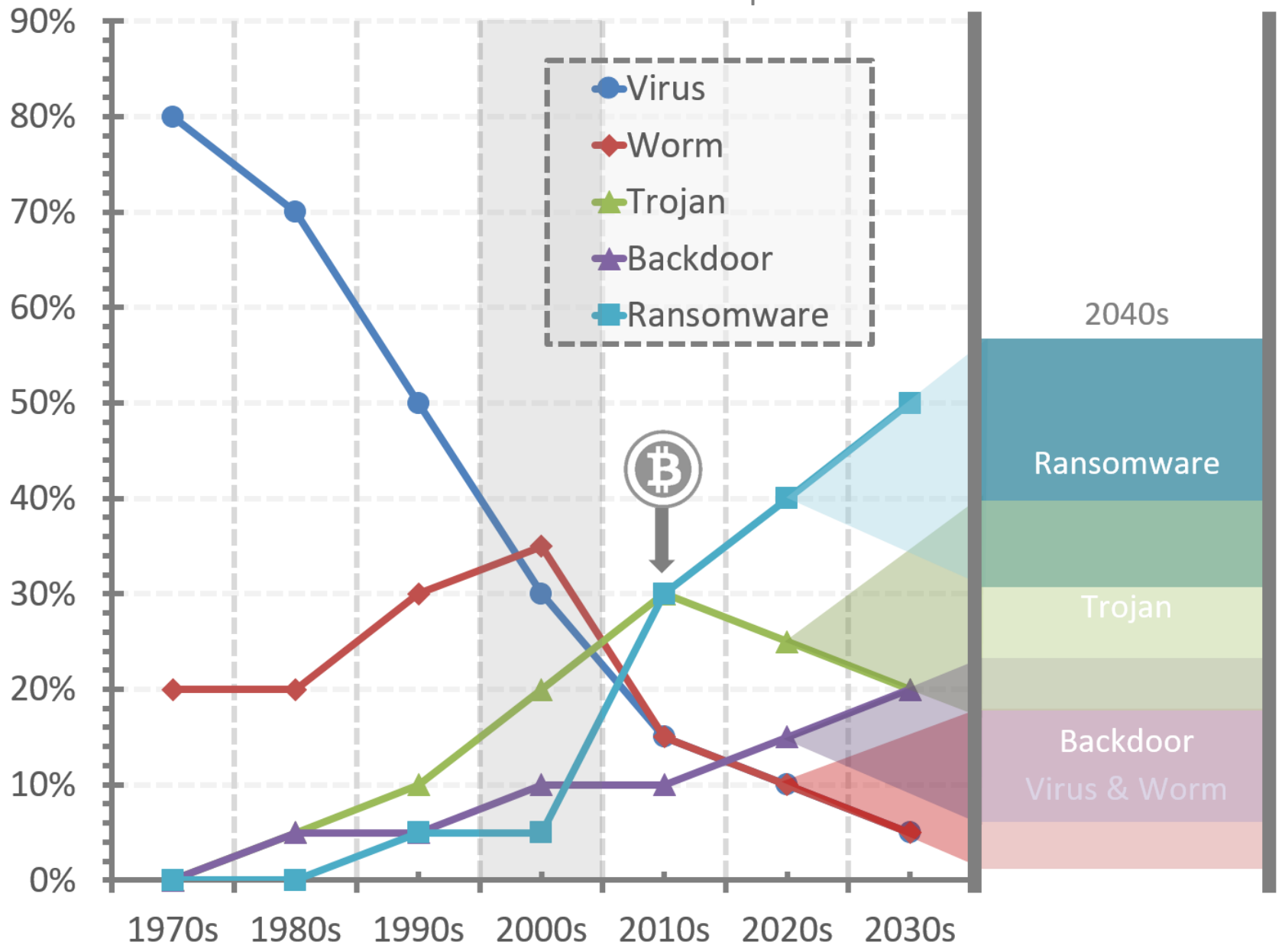
Virus: 30%
(Încă frecvent, dar
umbrit de noi amenințări)

Worm: 35%
(Vârful activităților worm
cu focare globale majore)

Trojan: 20%
(Creștere semnificativă
în sofisticare și prevalență)

Backdoor: 10%
(Utilizat în ciber-spionaj
mai complex)

Ransomware: 5%
(Emergența
ransomware-ului modern)



Tipuri de malware/Decada

Distributia aproximativa:

Apar criptomonezi:
- Incontrolabile – identitate necunoscuta.
- Independent de sistemul bancar.

Anii 2010

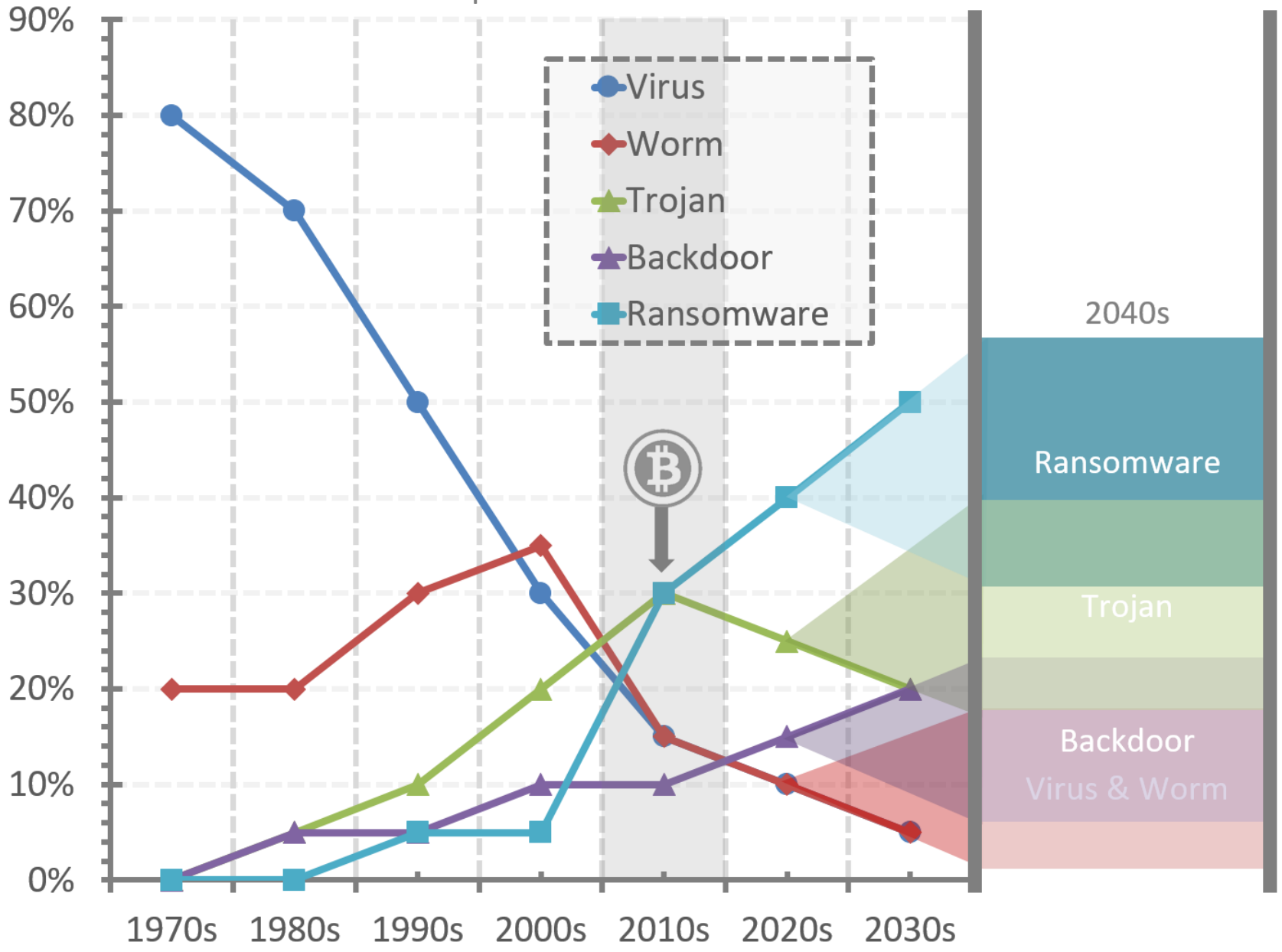
Virus: 15%
(Eclipsat de tipuri de malware mai sofisticate)

Worm: 15%
(Încă prezent, dar mai puțin dominant)

Trojan: 30%
(Semnificativ sub forma APT-urilor și troienilor bancari)

Backdoor: 10%
(În special în atacuri sponsorizate de stat)

Ransomware: 30%
(Creștere rapidă cu atacuri de mare profil)



Tipuri de malware/Decada

Distributia aproximativa:

Adaptarea la criptomonezi:
- Reutilizarea malware pentru şantaj.
- Ascendent doar Ransomeware si Backdoor.

Anii 2020

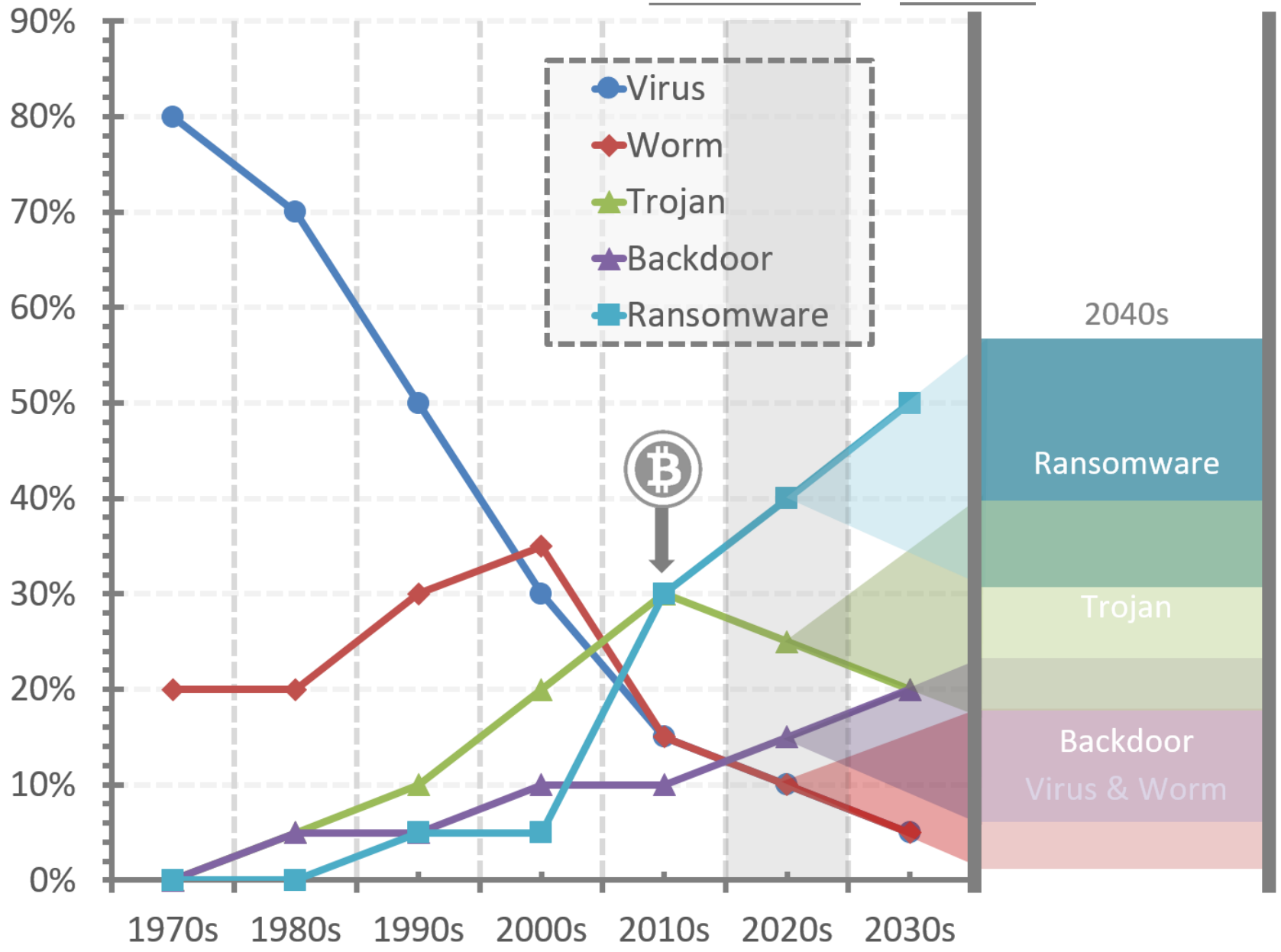
Virus: 10%
(Mai puțin comun
în sensul tradițional)

Worm: 10%
(Încă utilizat, dar nu
amenințarea principală)

Trojan: 25%
(Continuă să fie important,
mai ales în atacuri țintite)

Backdoor: 15%
(Creștere în sofisticare
și utilizare în spionaj)

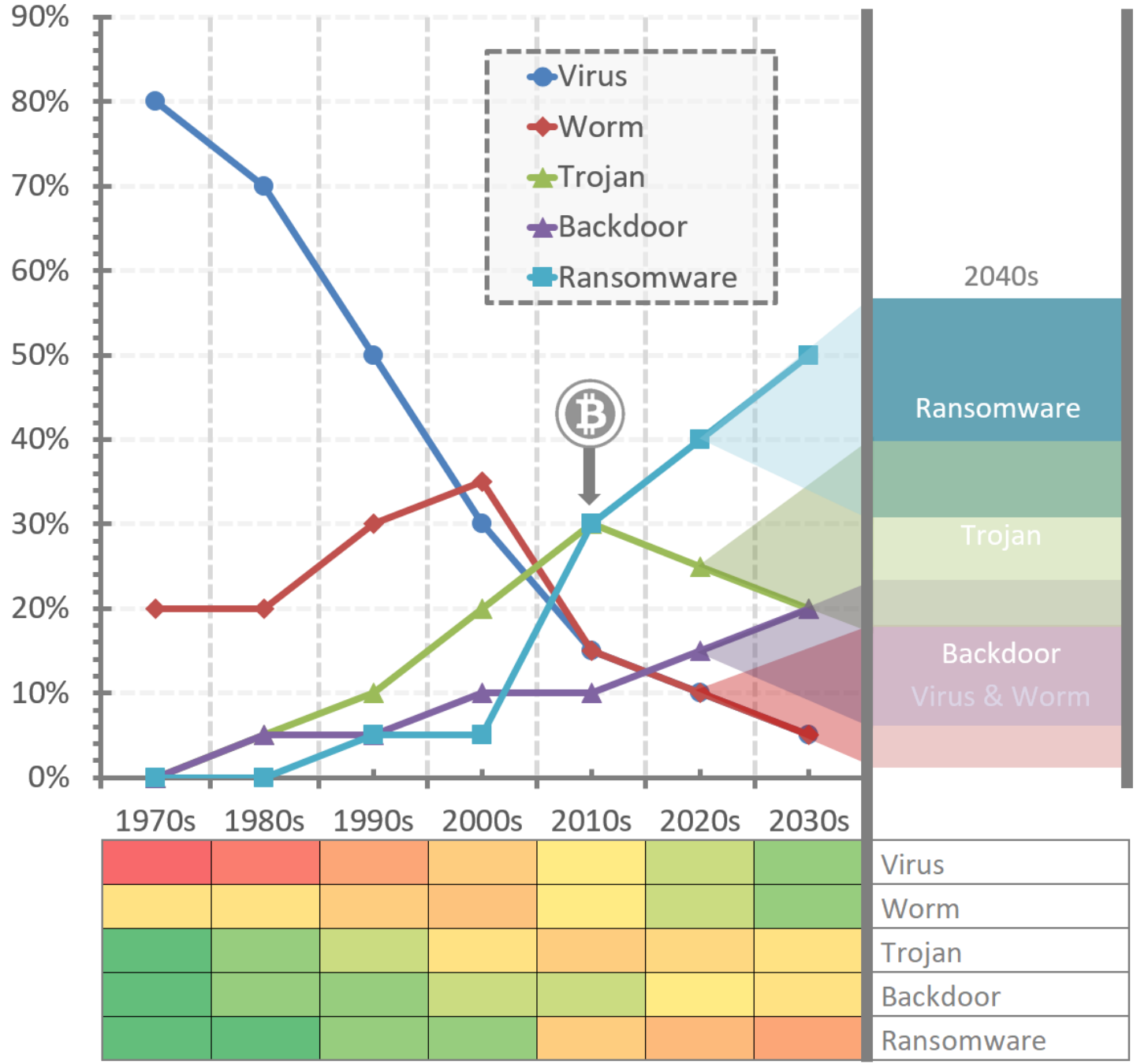
Ransomware: 40%
(Forma dominantă de
malware în ultimii ani)



Tipuri de malware/Decada

Distributia aproximativa:

- Aceste procente sunt estimări generale și sunt supuse variațiilor bazate pe diferite surse de date și natura în evoluție a amenințărilor de securitate cibernetică.
- Acestea reprezintă un trend general în peisajul malware, de la virusuri simple auto-replicante la atacuri complexe sponsorizate de stat și ransomware motivat financiar.



Tipuri de malware/Decada

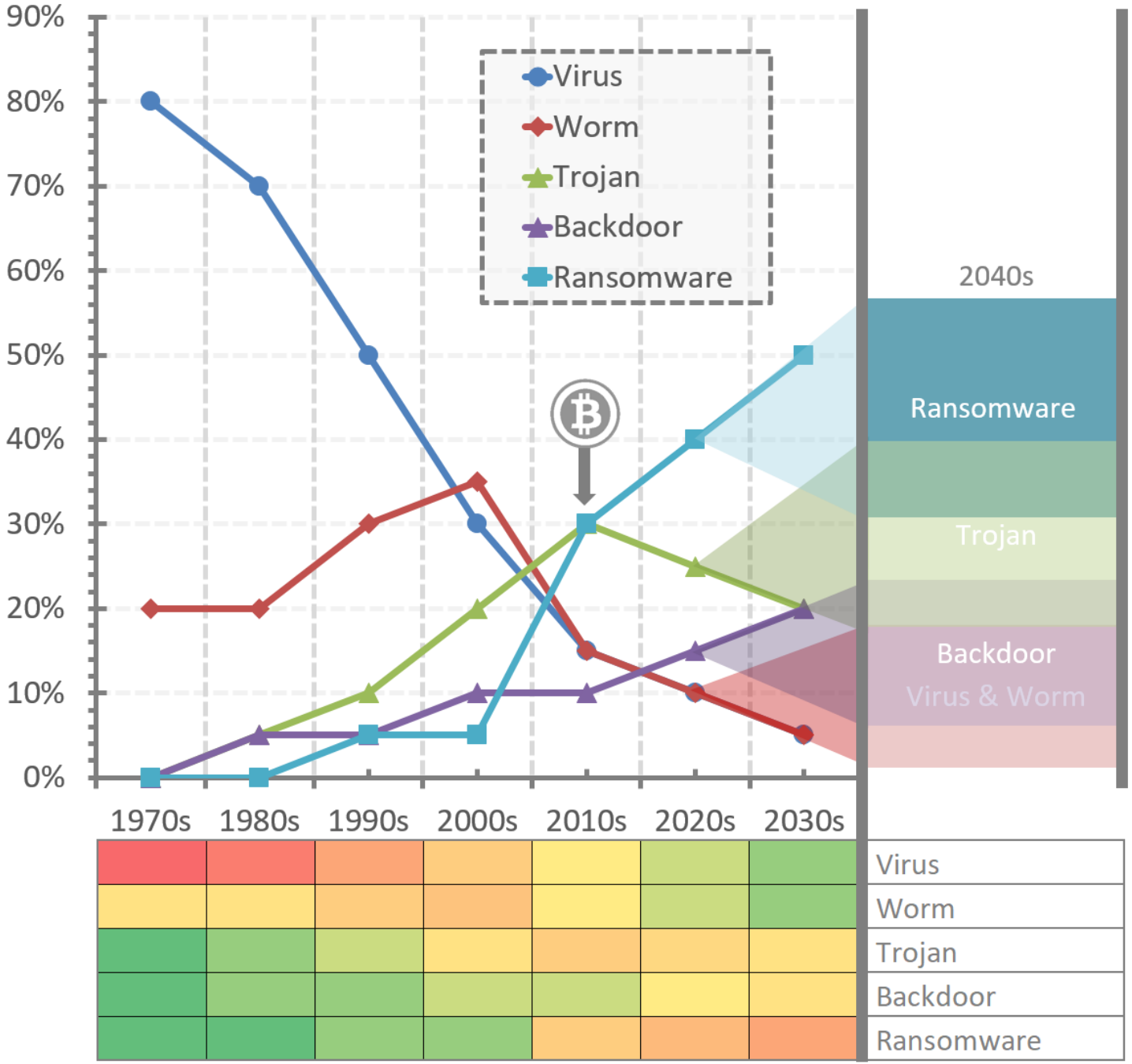
Distributia aproximativa:

- De ce nu mai observam viruși?

- OS mai vechi au fost eliminate treptat (procese izolate, restricții).
- Nimeni nu trimite fișiere executabile (email sau USB).
- Executabile trimise ca arhivă cu parolă (comportamentul forțat).

- De ce nu mai observam viermi?

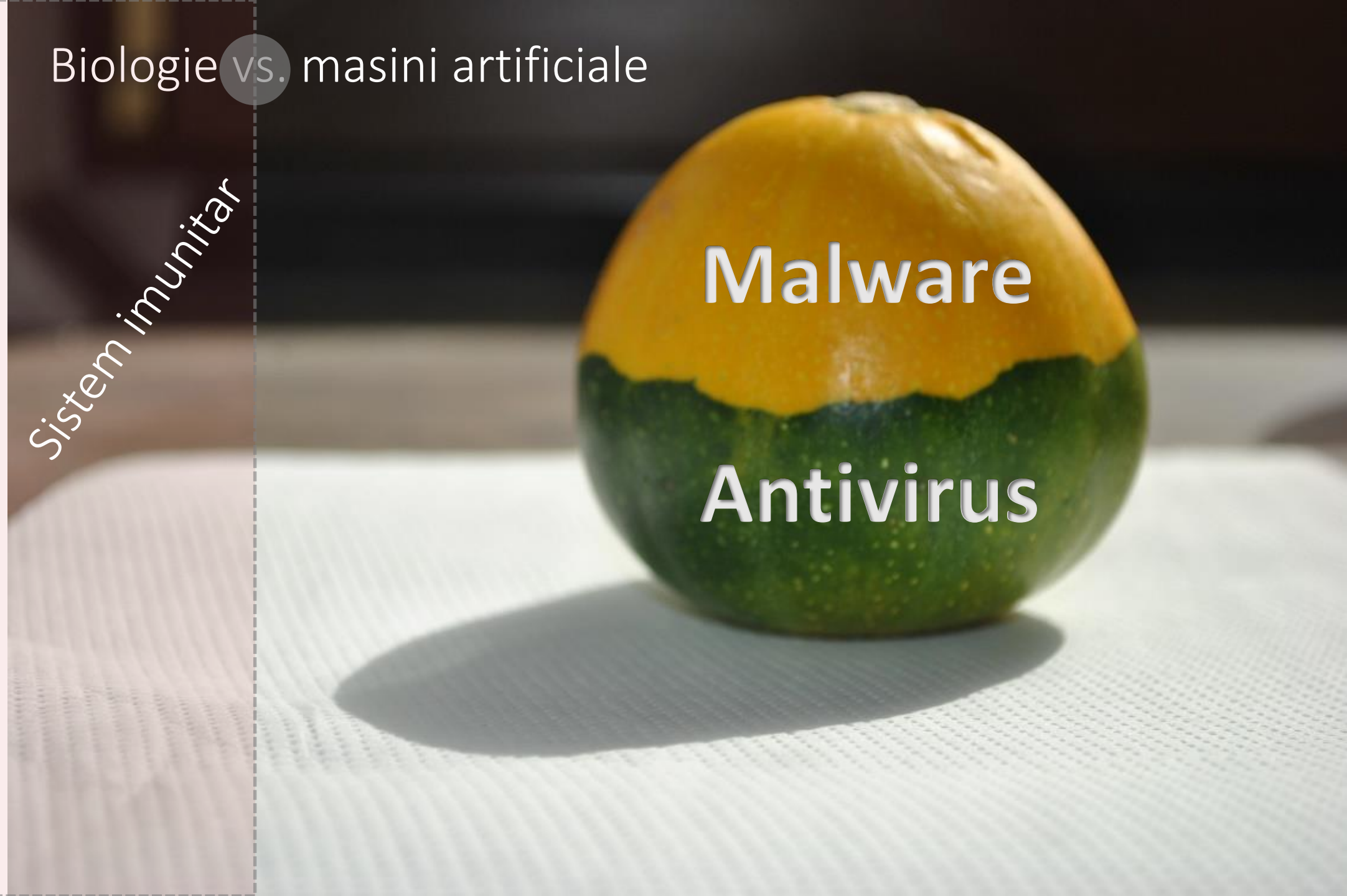
- Pool-ul de exploit-uri a fost parțial epuizat.
- Actualizarea OS în timp real închide ușor o potentiala vulnerabilitate.

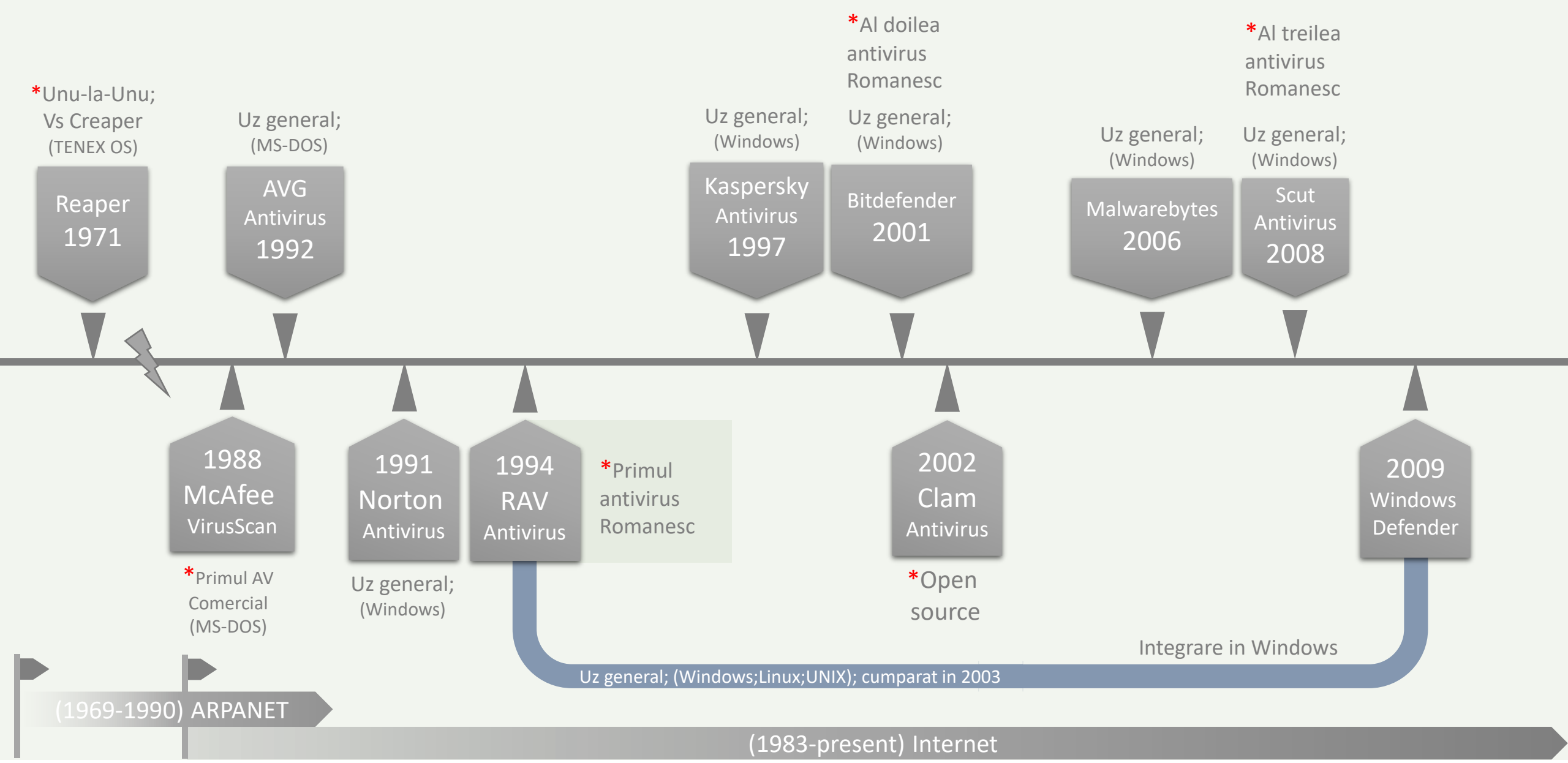


C.1.3
EVOLUȚIA SOLUȚIILOR DE SECURITATE

Biologie vs. masini artificiale

Sistem imunitar





Solutii antivirus !

Companiile AV serioase & discriminarea optima.

1970 - 2010

```
cmp   cl,40h
jae   7C901B1C
cmp   cl,20h
jae   7C901B12
shld  edx,eax,cl
shl   eax,cl
ret
mov   edx,eax
xor   eax,eax
and   cl,1Fh
shl   edx,cl
ret
xor   eax,eax
xor   edx,edx
```

IN HOC SIGNO VINCES

QUIS CUSTODIET IPSOS CUSTODES

CONSILIO ET PRUDENTIA

GLOBAL ADVANCED TECHNOLOGY

SCUT ANTI VIRUS

SCUT FAMILY SYSTEM INFORMATION SECURITY

Home | Defense Center | World Status | Download | Solutions | eStore | Products | Partners | Virus Encyclopedia | FAQ | About Novus Ordo

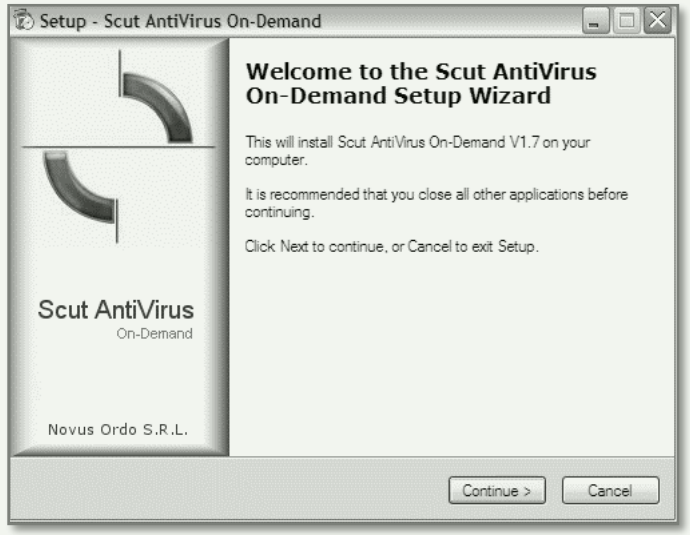
Whether you're at home or away, you can rest easy knowing that Scut Antivirus system is behind you. Antivirus professionals keep a constant, watchful eye on malware, spyware, crimeware, exploits and vulnerabilityes that are appearing every day around the globe. The proactive detection of Scut AntiVirus keeps a vigilant eye on your home and your business by constantly monitoring malware or spyware programs.

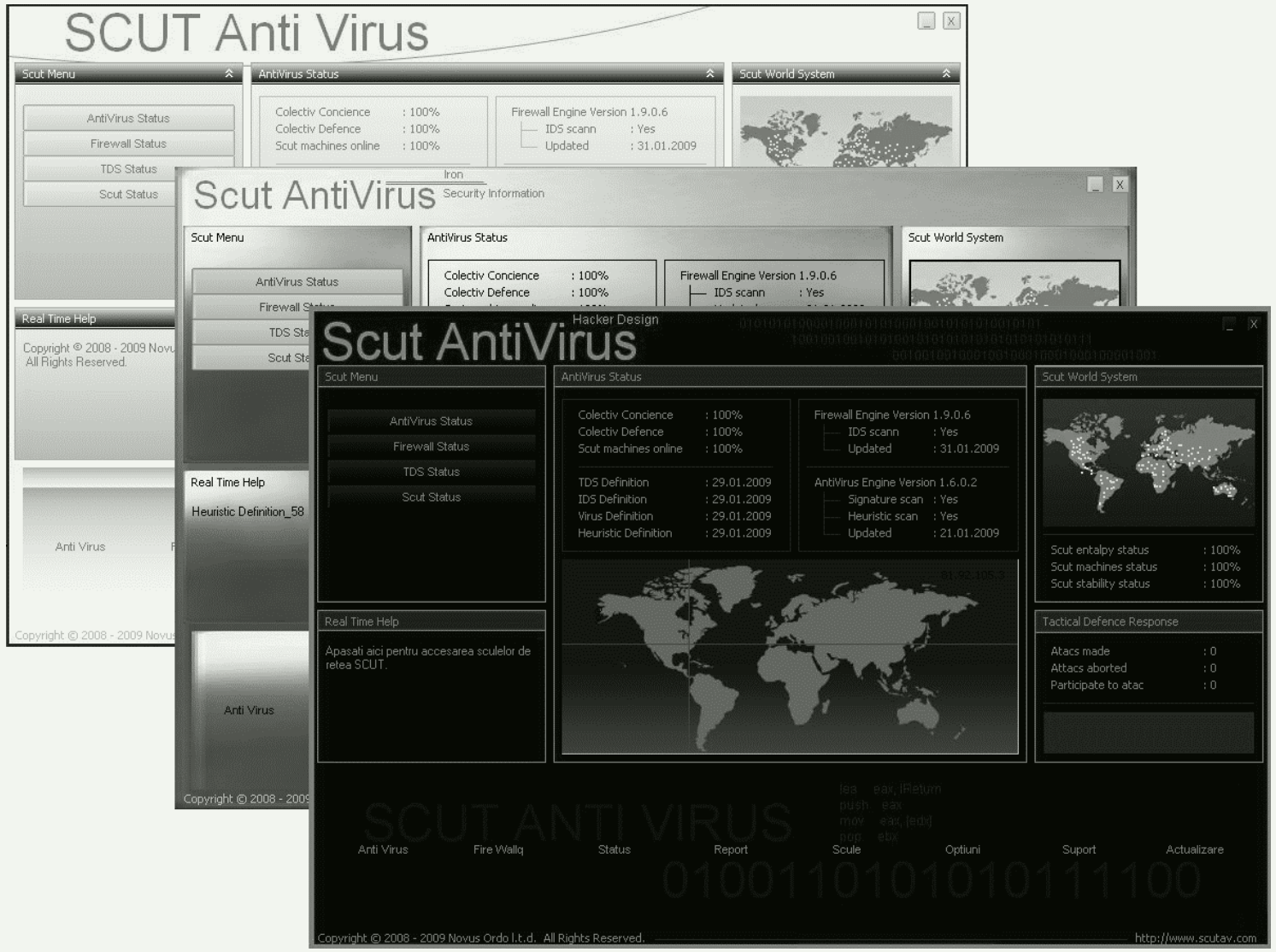
Scut AntiVirus scans your system for all types of malware, such as viruses, rootkits, trojans, keyloggers, spyware, adware etc. If the threat is detected, it can be easily removed from your computer.

Scut AntiVirus

Total Security

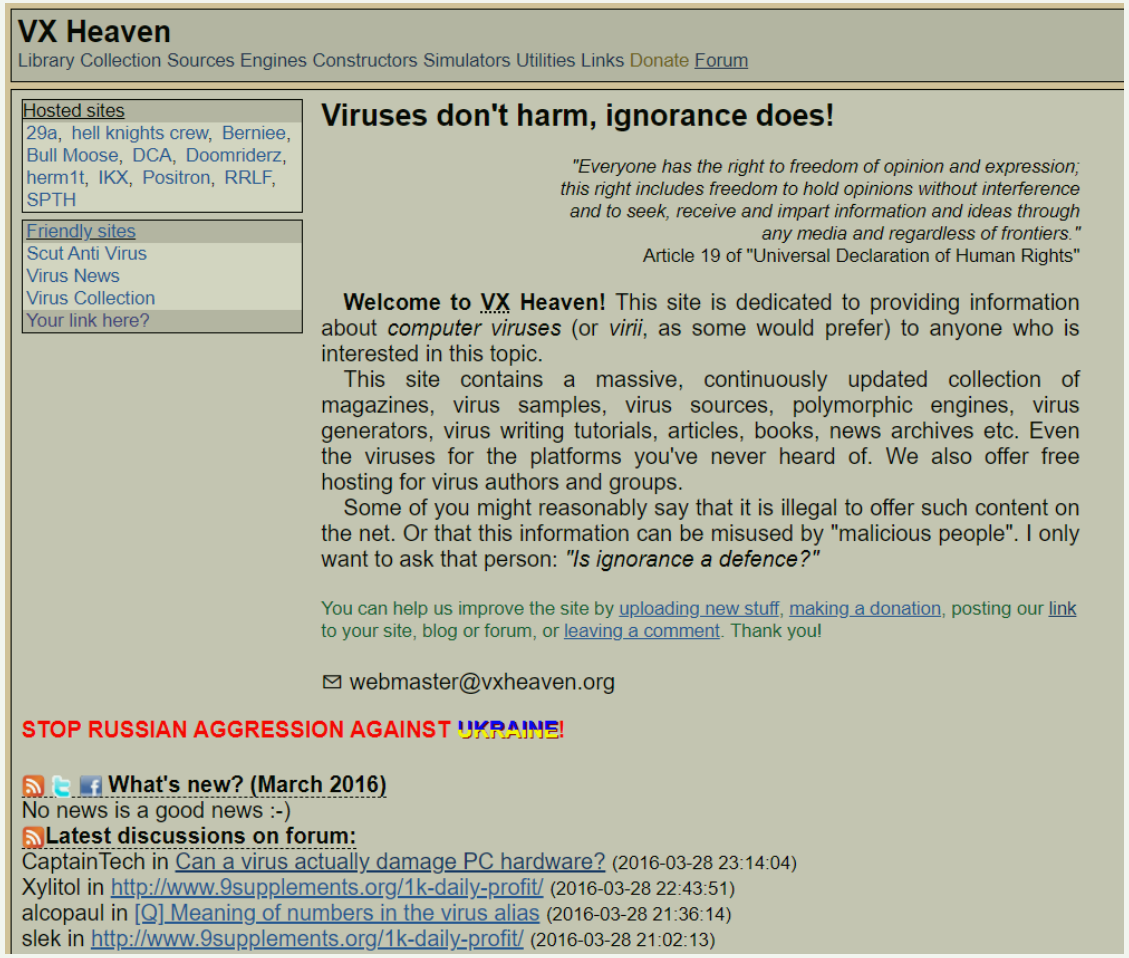
Puțin despre soluția *Scut Antivirus*





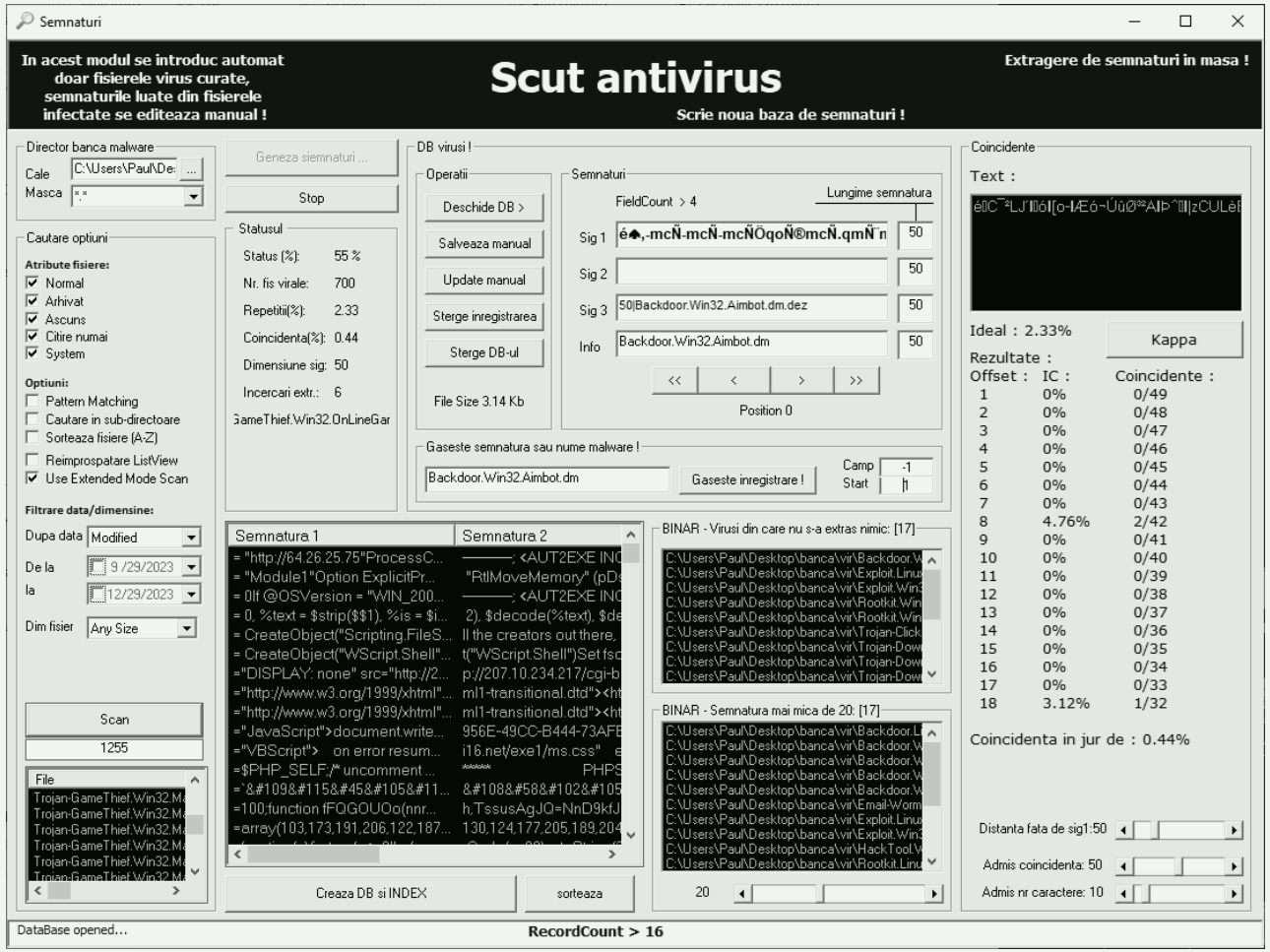
INTERNET ARCHIVE
WayBackMachine

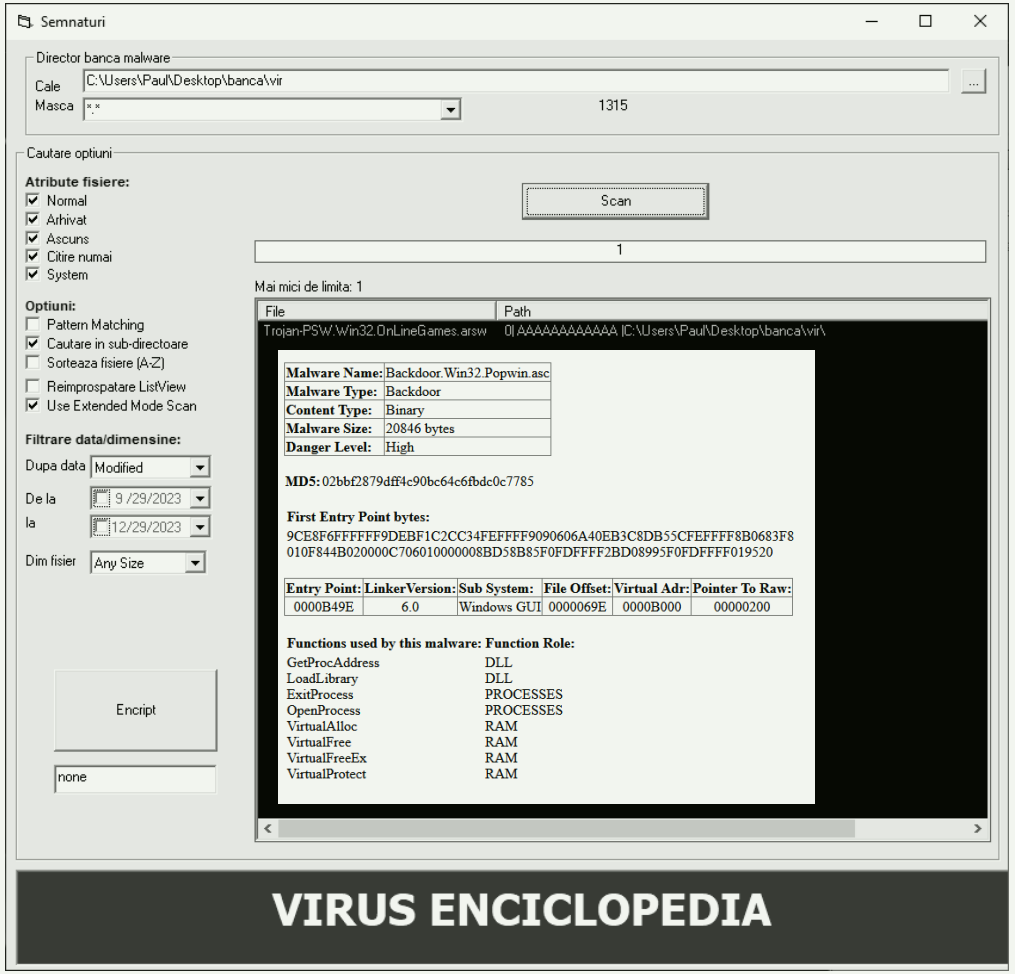
VX Heaven – Importanța băncilor malware!



Automatizare extragere de semnaturi

Scut AntiVirus



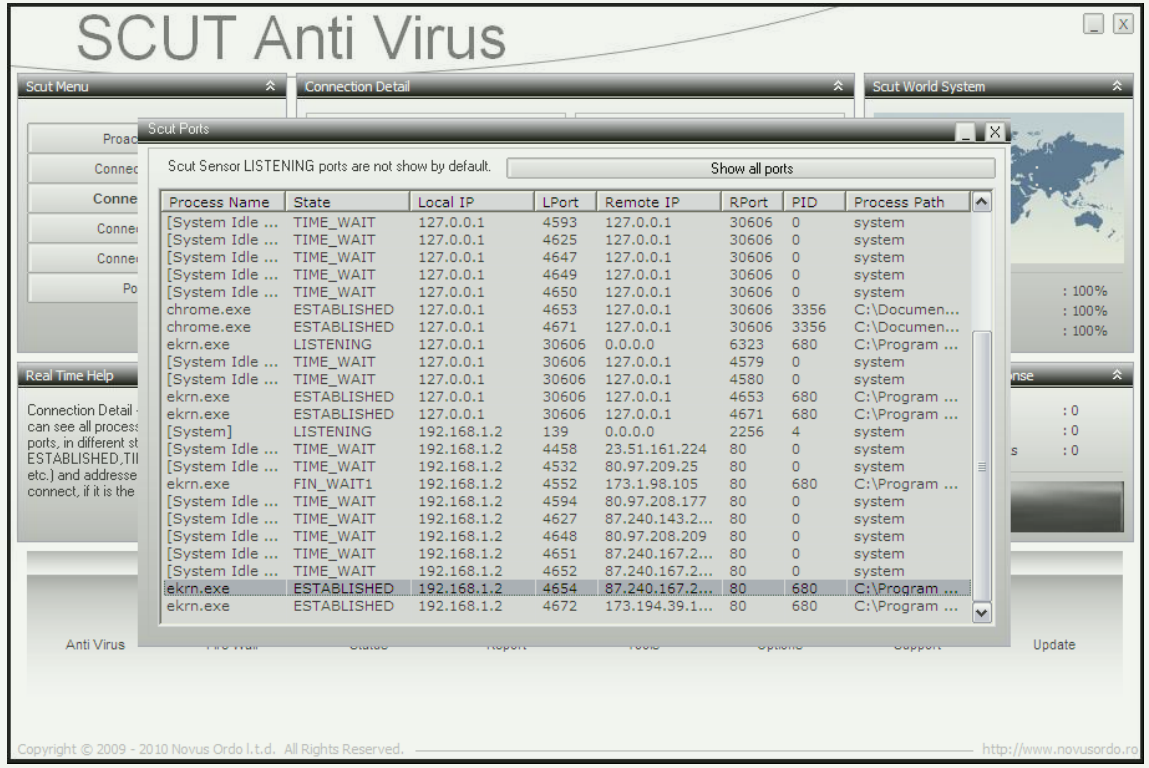


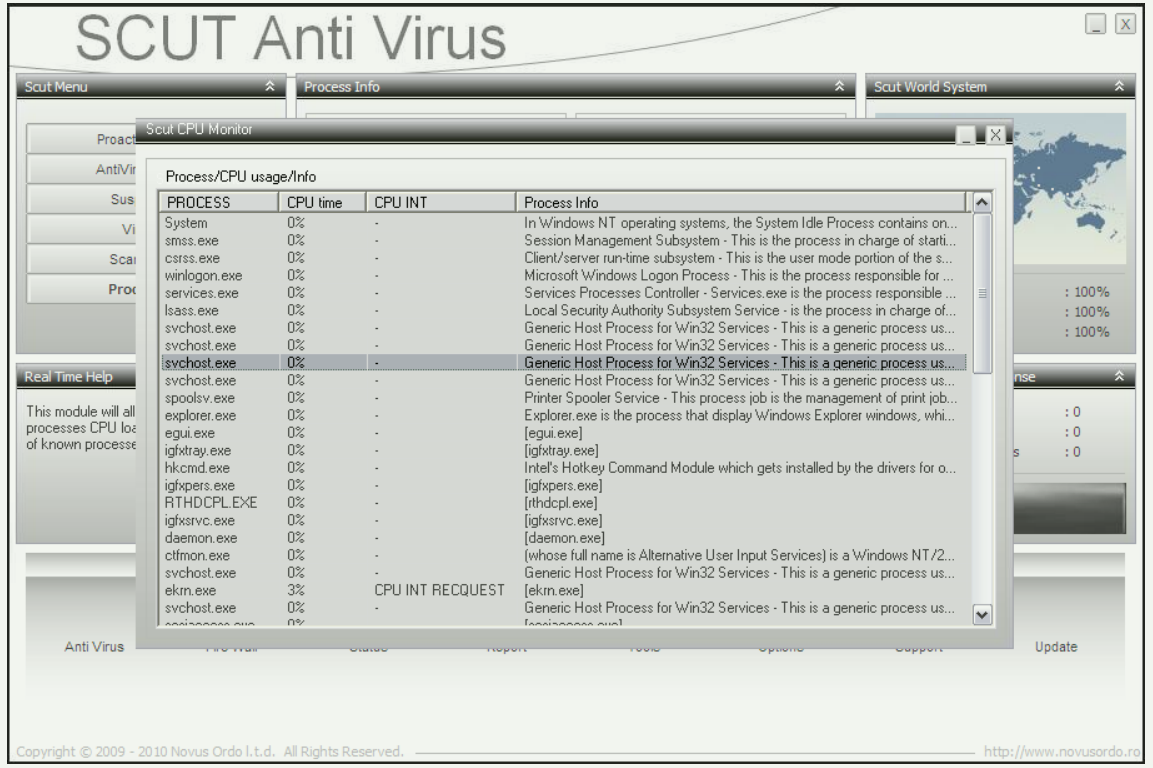
Puțin despre soluția *Scut Antivirus*

Scut AntiVirus

Termenul antivirus a prins rădăcini încă din anii 1980, când tipul majoritar de malware era virusul.

Astăzi acest termen (i.e. “antivirus”) este încă folosit datorită respectului cuvenit experților în securitate care au fost pionierii sistemului imunitar artificial pe care îl avem astăzi.



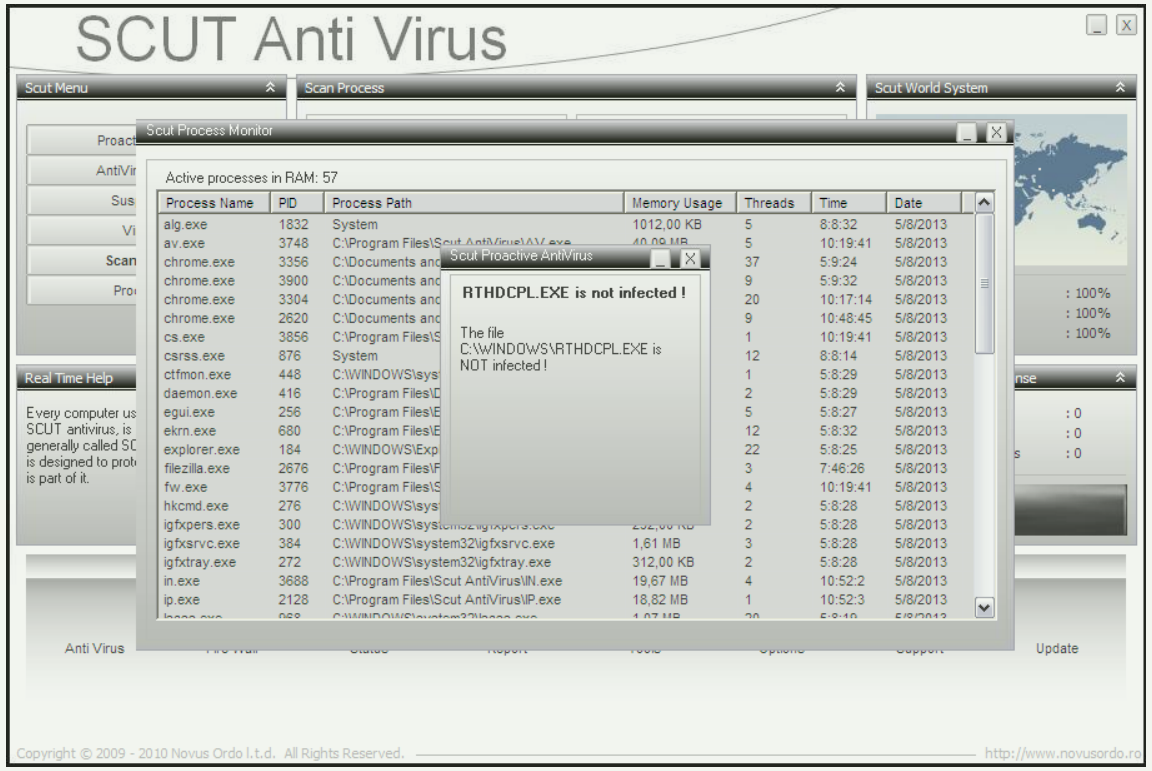


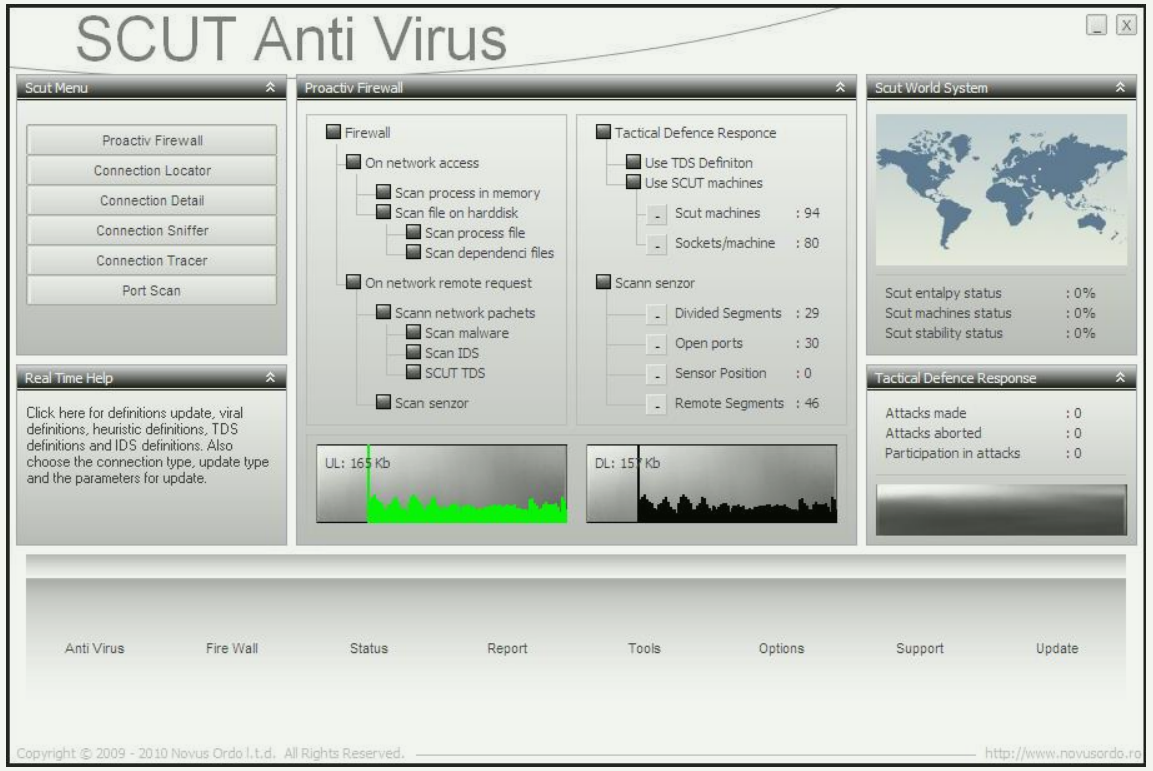
Puțin despre soluția *Scut Antivirus*

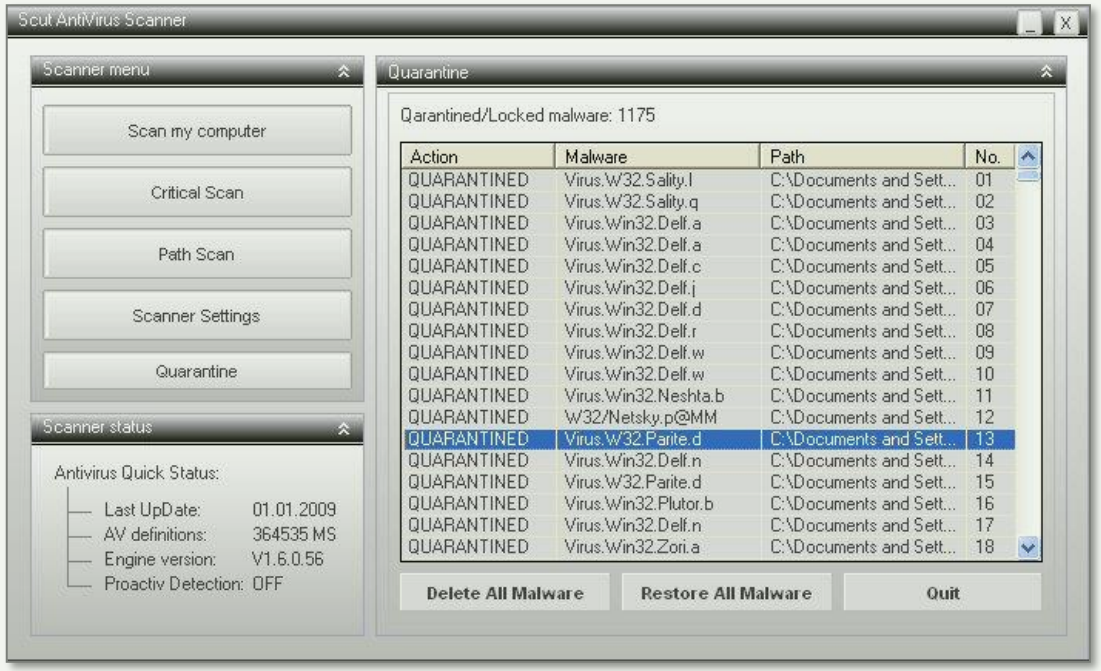
Scut AntiVirus

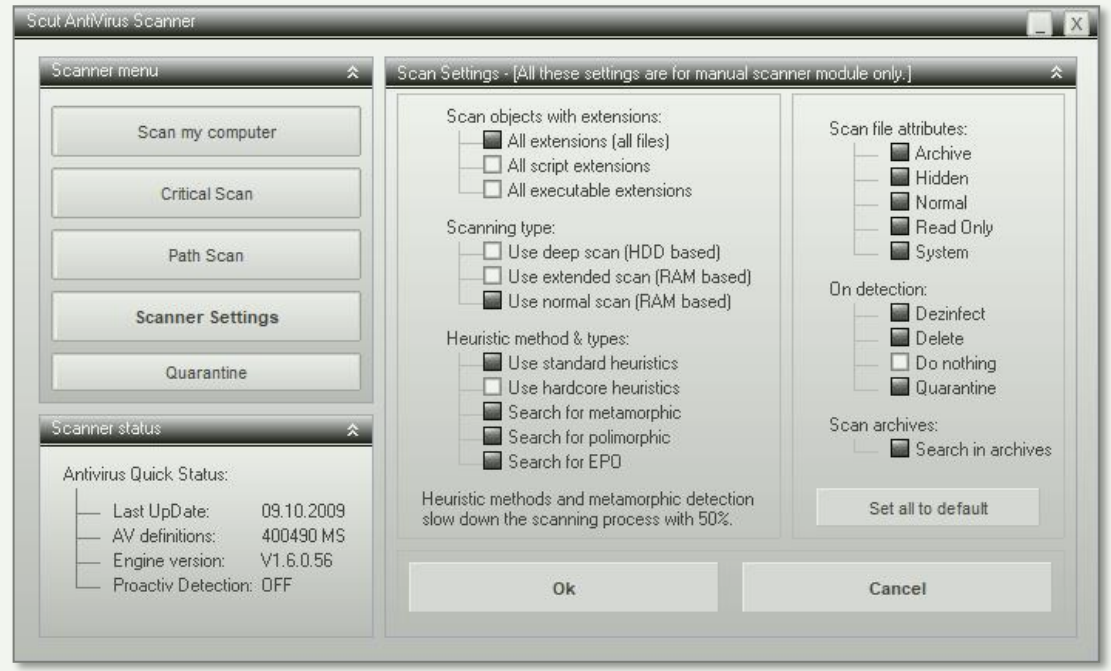
Termenul antivirus a prins rădăcini încă din anii 1980, când tipul majoritar de malware era virusul.

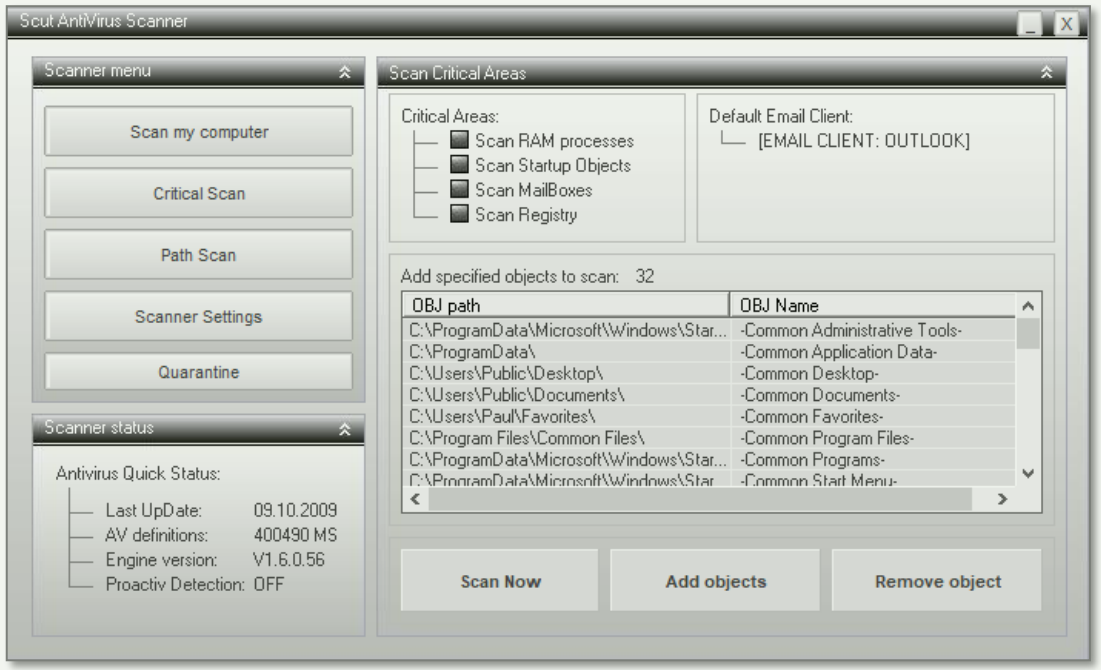
Astăzi acest termen (i.e. “antivirus”) este încă folosit datorită respectului cuvenit experților în securitate care au fost pionierii sistemului imunitar artificial pe care îl avem astăzi.

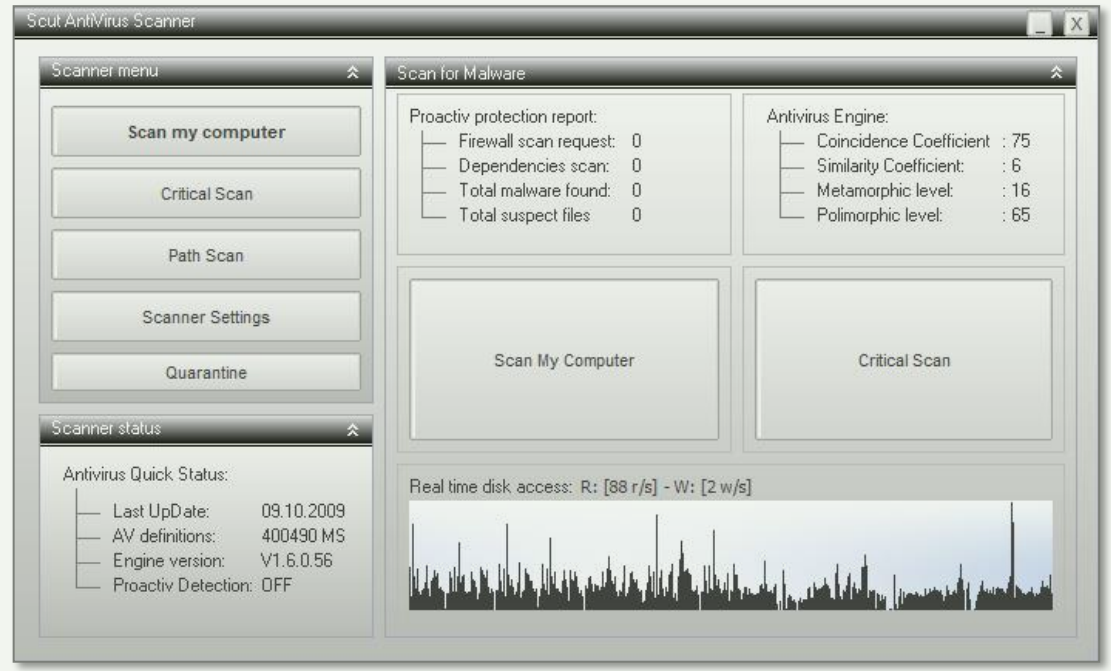





Scut AntiVirus Scanner
Scanner menu
Scan my computer
Critical Scan
Path Scan
Scanner Settings
Quarantine
Scanner status
Antivirus Quick Status:
Last UpDate: 01.01.2009
AV definitions: 364535 MS
Engine version: V1.6.0.56
Proactiv Detection: OFF
Quarantine
Qarantined/Locked malware: 1175
Action | Malware | Path | No.
QUARANTINED | Virus.W32.Sality.I | C:\Documents and Sett... | 01
QUARANTINED | Virus.W32.Sality.q | C:\Documents and Sett... | 02
QUARANTINED | Virus.Win32.Delf.a | C:\Documents and Sett... | 03
QUARANTINED | Virus.Win32.Delf.a | C:\Documents and Sett... | 04
QUARANTINED | Virus.Win32.Delf.c | C:\Documents and Sett... | 05
QUARANTINED | Virus.Win32.Delf.j | C:\Documents and Sett... | 06
QUARANTINED | Virus.Win32.Delf.d | C:\Documents and Sett... | 07
QUARANTINED | Virus.Win32.Delf.r | C:\Documents and Sett... | 08
QUARANTINED | Virus.Win32.Delf.w | C:\Documents and Sett... | 09
QUARANTINED | Virus.Win32.Delf.w | C:\Documents and Sett... | 10
QUARANTINED | Virus.Win32.Neshta.b | C:\Documents and Sett... | 11
QUARANTINED | W32/Netsky.p@MM | C:\Documents and Sett... | 12
QUARANTINED | Virus.W32.Parite.d | C:\Documents and Sett... | 13
QUARANTINED | Virus.Win32.Delf.n | C:\Documents and Sett... | 14
QUARANTINED | Virus.W32.Parite.d | C:\Documents and Sett... | 15
QUARANTINED | Virus.Win32.Plutor.b | C:\Documents and Sett... | 16
QUARANTINED | Virus.Win32.Delf.n | C:\Documents and Sett... | 17
QUARANTINED | Virus.Win32.Zori.a | C:\Documents and Sett... | 18
Delete All Malware
Restore All Malware
Quit


Scut AntiVirus Scanner
Scanner menu
Scan my computer
Critical Scan
Path Scan
Scanner Settings
Quarantine
Scanner status
Antivirus Quick Status:
Last UpDate: 09.10.2009
AV definitions: 400490 MS
Engine version: V1.6.0.56
Proactiv Detection: OFF
Scan Settings - [All these settings are for manual scanner module only.]
Scan objects with extensions:
All extensions (all files)
All script extensions
All executable extensions
Scanning type:
Use deep scan (HDD based)
Use extended scan (RAM based)
Use normal scan (RAM based)
Heuristic method & types:
Use standard heuristics
Use hardcore heuristics
Search for metamorphic
Search for polimorphic
Search for EPO
Heuristic methods and metamorphic detection slow down the scanning process with 50%.
Scan file attributes:
Archive
Hidden
Normal
Read Only
System
On detection:
Dezinfect
Delete
Do nothing
Quarantine
Scan archives:
Search in archives
Set all to default
Ok
Cancel


Scut AntiVirus Scanner
Scanner menu
Scan my computer
Critical Scan
Path Scan
Scanner Settings
Quarantine
Scanner status
Antivirus Quick Status:
Last UpDate: 09.10.2009
AV definitions: 400490 MS
Engine version: V1.6.0.56
Proactiv Detection: OFF
Scan Critical Areas
Critical Areas:
Scan RAM processes
Scan Startup Objects
Scan MailBoxes
Scan Registry
Default Email Client:
[EMAIL CLIENT: OUTLOOK]
Add specified objects to scan: 32
OBJ path | OBJ Name
C:\ProgramData\Microsoft\Windows\Star... | -Common Administrative Tools-
C:\ProgramData\ | -Common Application Data-
C:\Users\Public\Desktop\ | -Common Desktop-
C:\Users\Public\Documents\ | -Common Documents-
C:\Users\Paul\Favorites\ | -Common Favorites-
C:\Program Files\Common Files\ | -Common Program Files-
C:\ProgramData\Microsoft\Windows\Star... | -Common Programs-
Scan Now
Add objects
Remove object


Scut AntiVirus Scanner
Scanner menu
Scan my computer
Critical Scan
Path Scan
Scanner Settings
Quarantine
Scanner status
Antivirus Quick Status:
Last UpDate: 09.10.2009
AV definitions: 400490 MS
Engine version: V1.6.0.56
Proactiv Detection: OFF
Scan for Malware
Proactiv protection report:
Firewall scan request: 0
Dependencies scan: 0
Total malware found: 0
Total suspect files 0
Antivirus Engine:
Coincidence Coefficient : 75
Similarity Coefficient: : 6
Metamorphic level: : 16
Polimorphic level: : 65
Scan My Computer
Critical Scan
Real time disk access: R: [88 r/s] - W: [2 w/s]

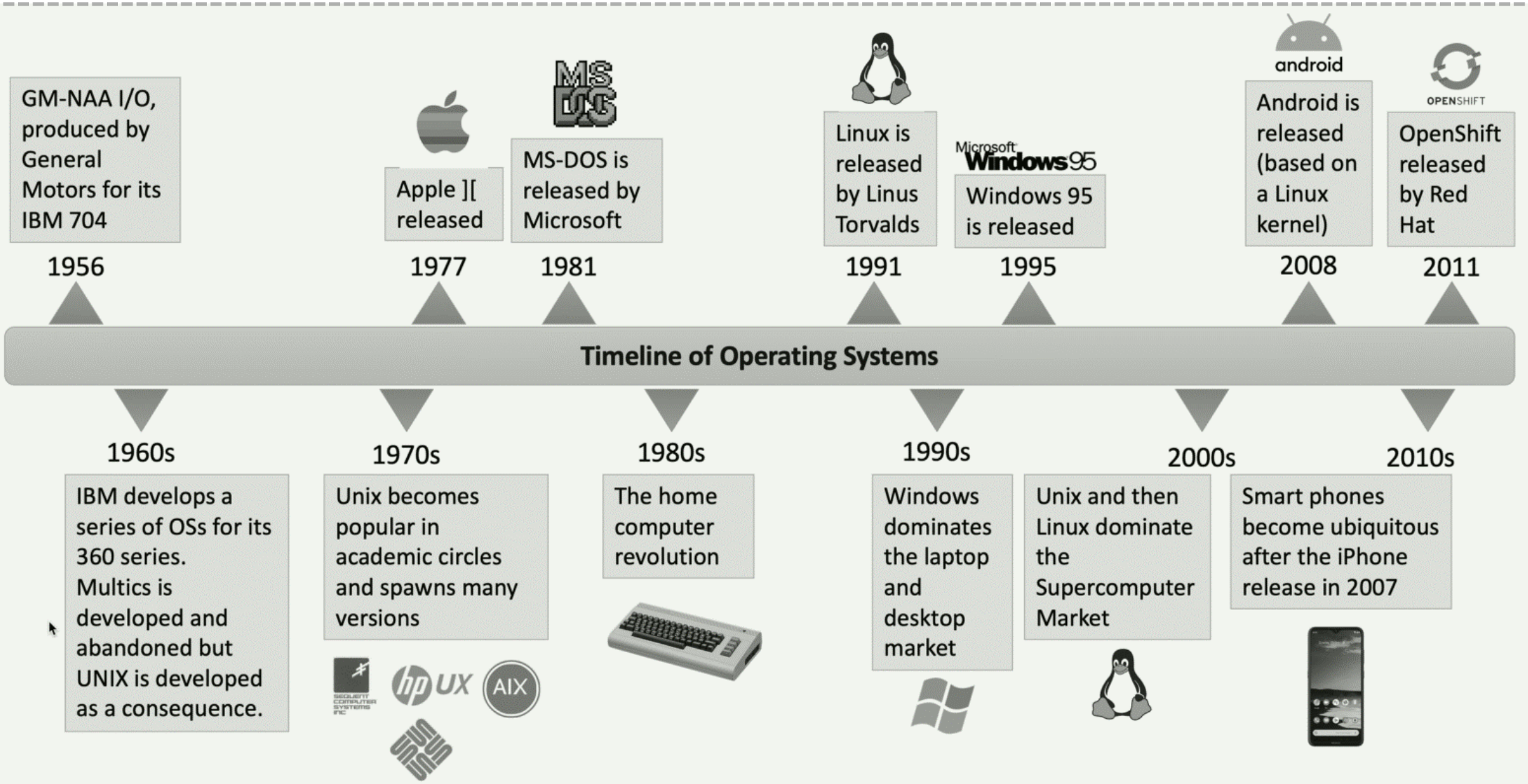
Puțin despre soluția *Scut Antivirus*

Scut AntiVirus

Chaaaatttttttttttttt10010001100101001010 …
GPTTTTTTTTTT0100110001010010010 …

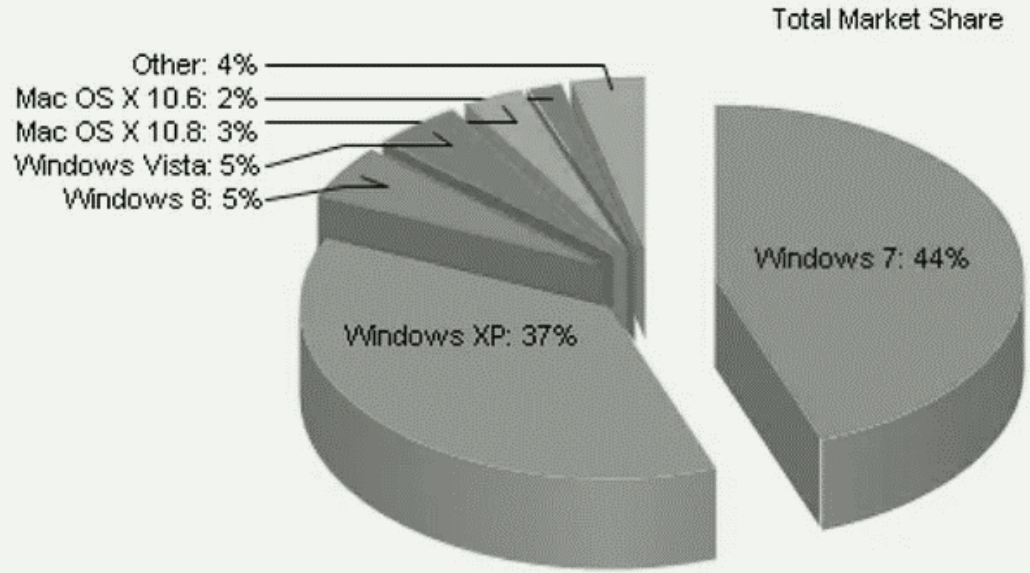
C.1.4
SISTEMELE DE OPERARE ȘI STRATUL DE PORTABILITATE

Sistemele de operare în timp

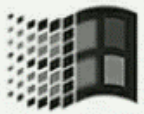


Windows Operating Systems

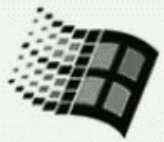
VERSION RELEASE DATE AND LIFECYCLE



Windows1
1985



Windows 3.1
1992



Windows 95
1995

Windows XP
2001

Windows
Vista 2006

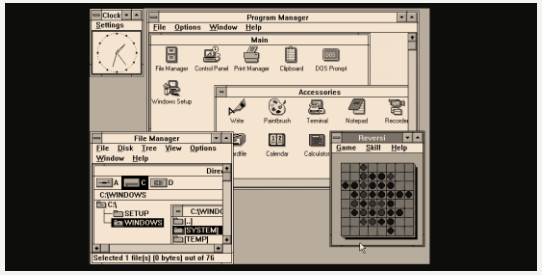
Windows 7
2009

Windows 8
2012

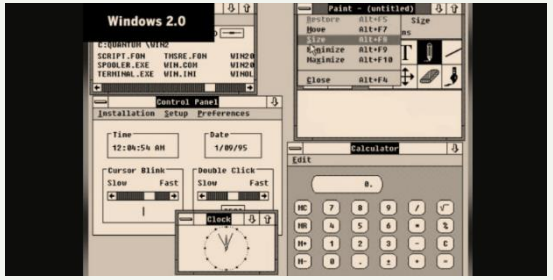
Windows 10
2015

Structura OS a dictat varianta de malware

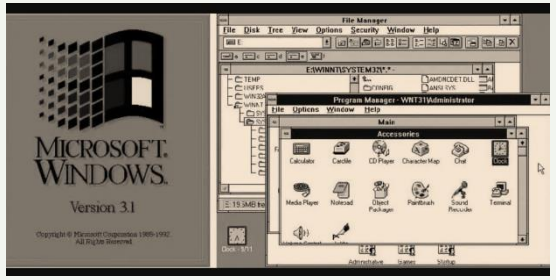
Windows 1



Windows 2.0

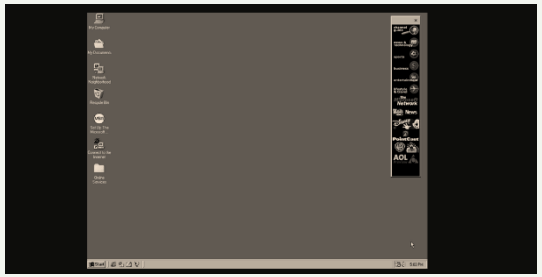


Windows 3.1

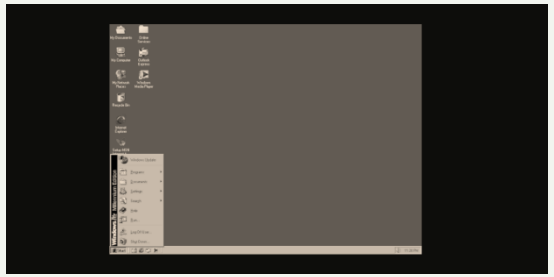


Windows 95

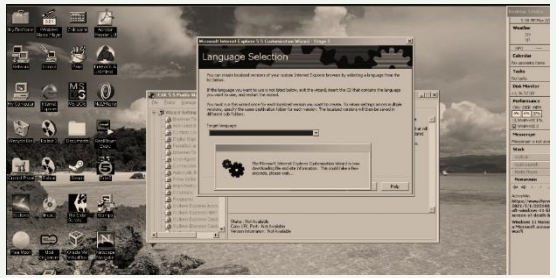
Windows 98



Windows 2000



Windows NT



Windows XP

Windows 7

Windows Vista

Windows 8.0

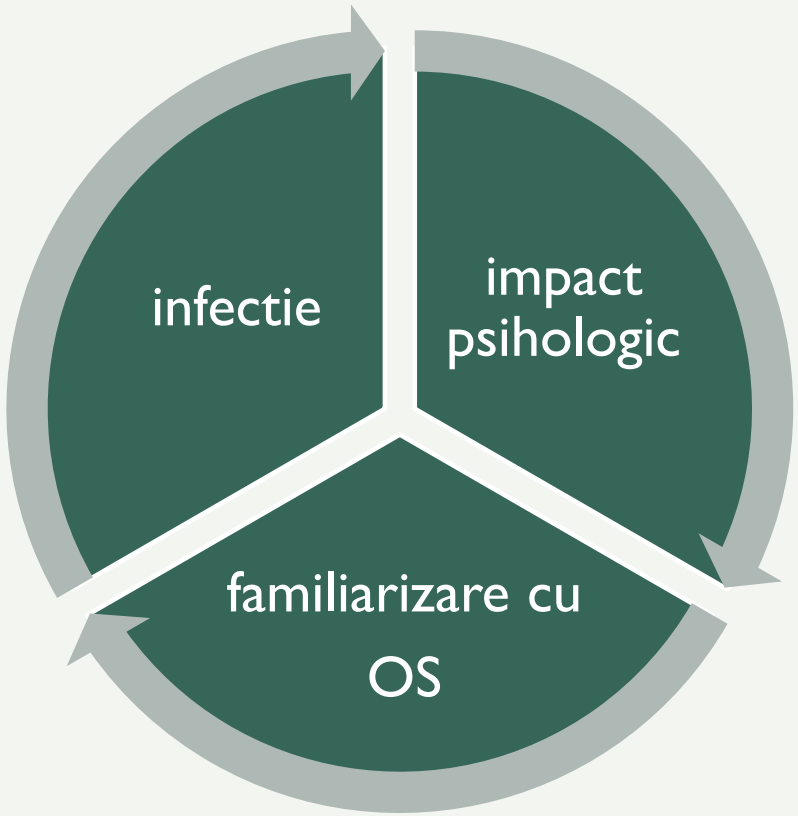
Windows 10

PERSISTENȚA SISTEMULUI DE OPERARE WINDOWS

RESPECTAREA LEGILOR NATURII

In masinile biologice, virus+host=evolutie

- Sistemele de operare care nu pot fi infectate, dispar!
- Infecția este o metodă evolutivă de îmbunătățire a sistemului de operare.
- Infecția a implicat utilizatorul din punct de vedere psihologic!
- Utilizatorul se angajează și dedică timp sistemului de operare pentru a afla mai multe despre cum funcționează.
- Omul revine la sistemul de operare pe care îl cunoaște!



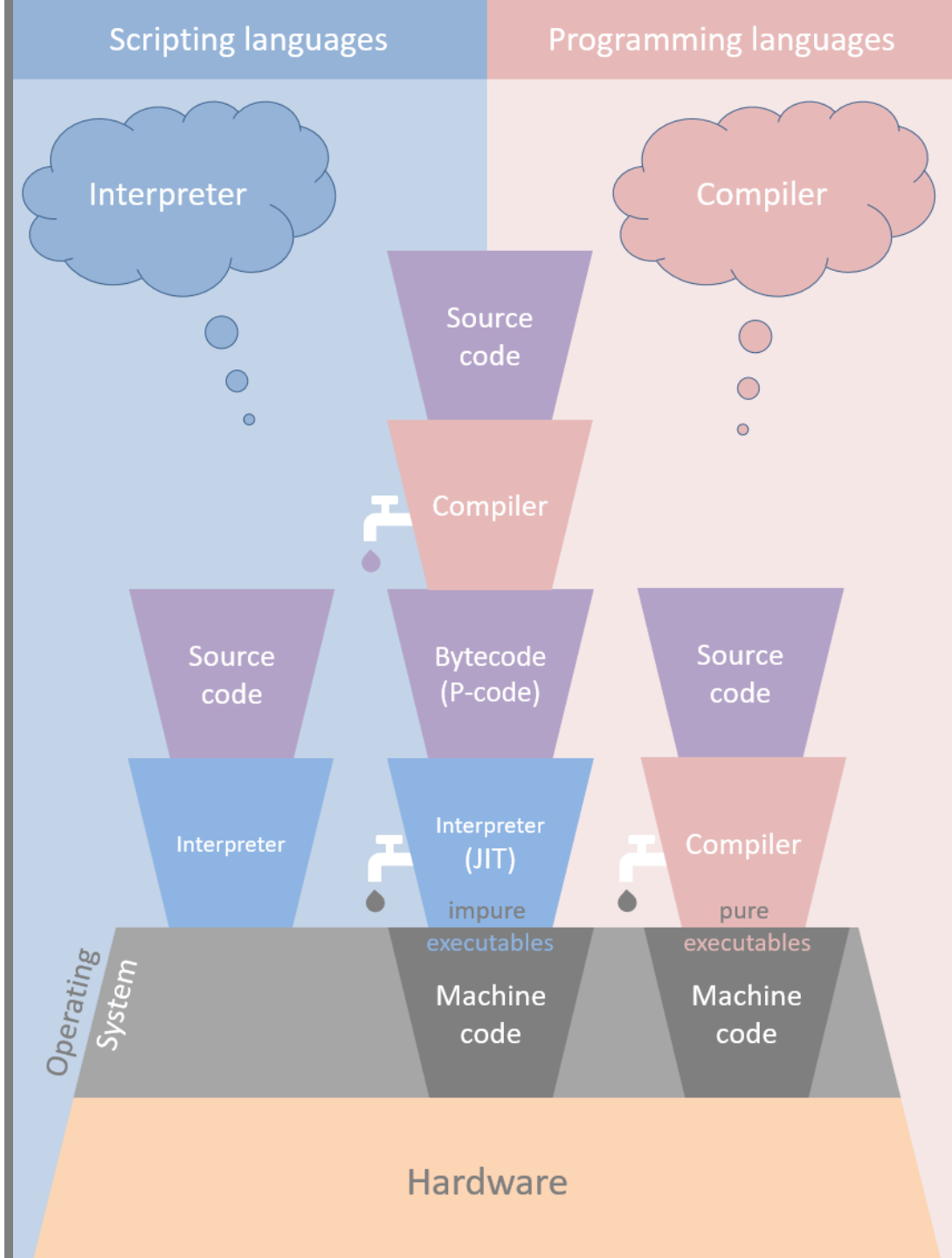
De ce ransomware este viitorul malware?

- Șurubul este strâns din punct de vedere al securității la nivel fundamental. Cum?:
- Sistem hybrid !

Se face distincția intre:

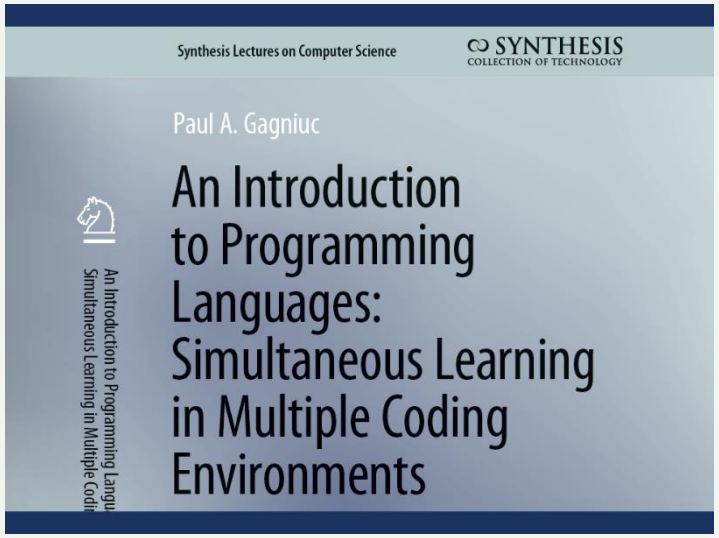
- Executabil – self (nativ)
- Executabil - non-self (hibrid)

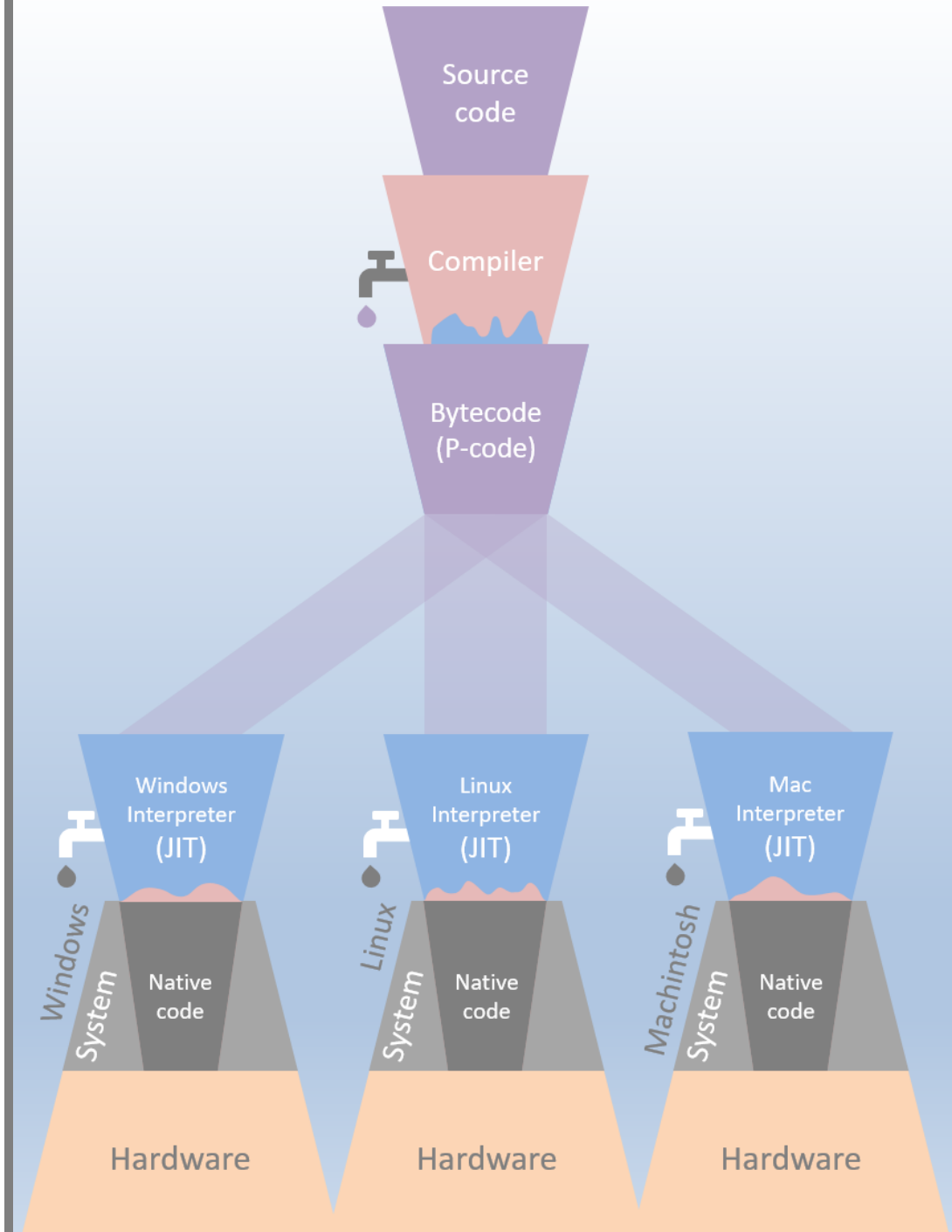
- Dezavantajul:
- Sistemul hibrid rămâne mediocru.
- Malware devine multi OS dar va fi non-self.



Direcția organizării software

- Universalitate:
- Limbaje de programare moderne
- Execuție pe mașini virtuale
- Portabilitatea aplicației



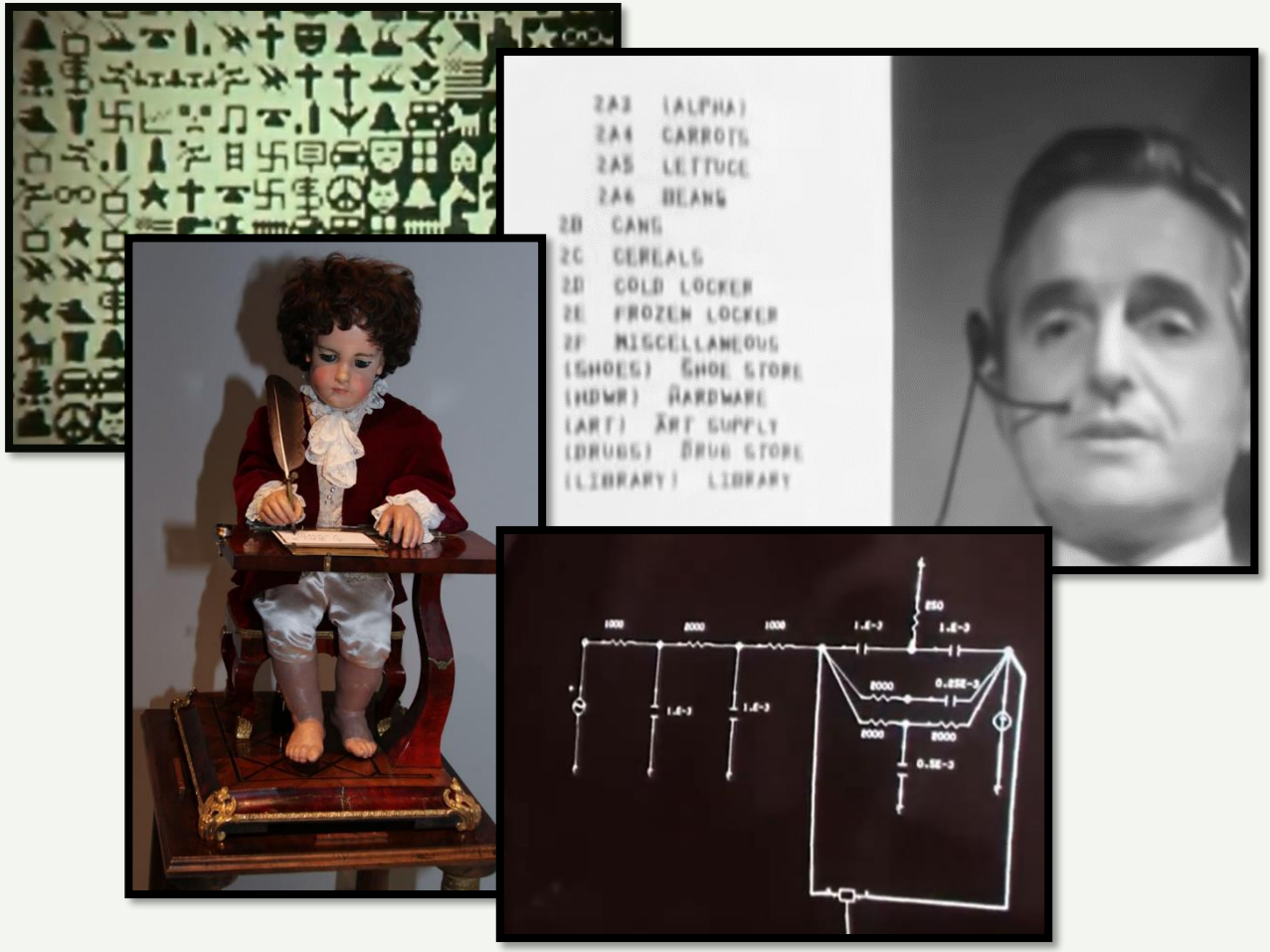


CONCLUZII

- Istoria calculatoarelor.
- Istoricul malware-ului și al soluțiilor de securitate.
- Evoluția tipurilor de malware.
- Evoluția sistemelor de operare, în special al Windows OS.
- Impactul psihologic al aplicațiilor malware asupra populației.
- Impactul sistemelor de operare asupra tipurilor de malware.

LINK-URI VIDEO RELEVANTE

- The Writer Automaton (1774)
- Mother of All Demos - 1968 (1/3)
- Mother of All Demos - 1968 (2/3)
- Mother of All Demos - 1968 (3/3)
- The Incredible Machine (1968)



BIBLIOGRAFIE / RESURSE

- Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.
- Paul A. Gagniuc. *An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments. Synthesis Lectures on Computer Science*. Springer International Publishing, 2023, pp. 1-280.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in MATLAB*, Springer, 2024, pp. 1-255.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Python*, Springer, 2024, pp. 1-245.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Javascript*, Springer, 2024, pp. 1-240.
- Paul A. Gagniuc. *Markov chains: from theory to implementation and experimentation*. Hoboken, NJ, John Wiley & Sons, USA, 2017, ISBN: 978-1-119-38755-8.

https://github.com/gagniuc