

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 SOLUȚIILOR DE SECURITATE**
- **C.1.4 SISTEMELE DE OPERARE ȘI STRATUL DE PORTABILITATE**

C.1.1

ISTORIA MAŞINILOR ARTIFICIALE DE UZ GENERAL



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



- Prima mașină de țesut cu memorie binară pe carduri!

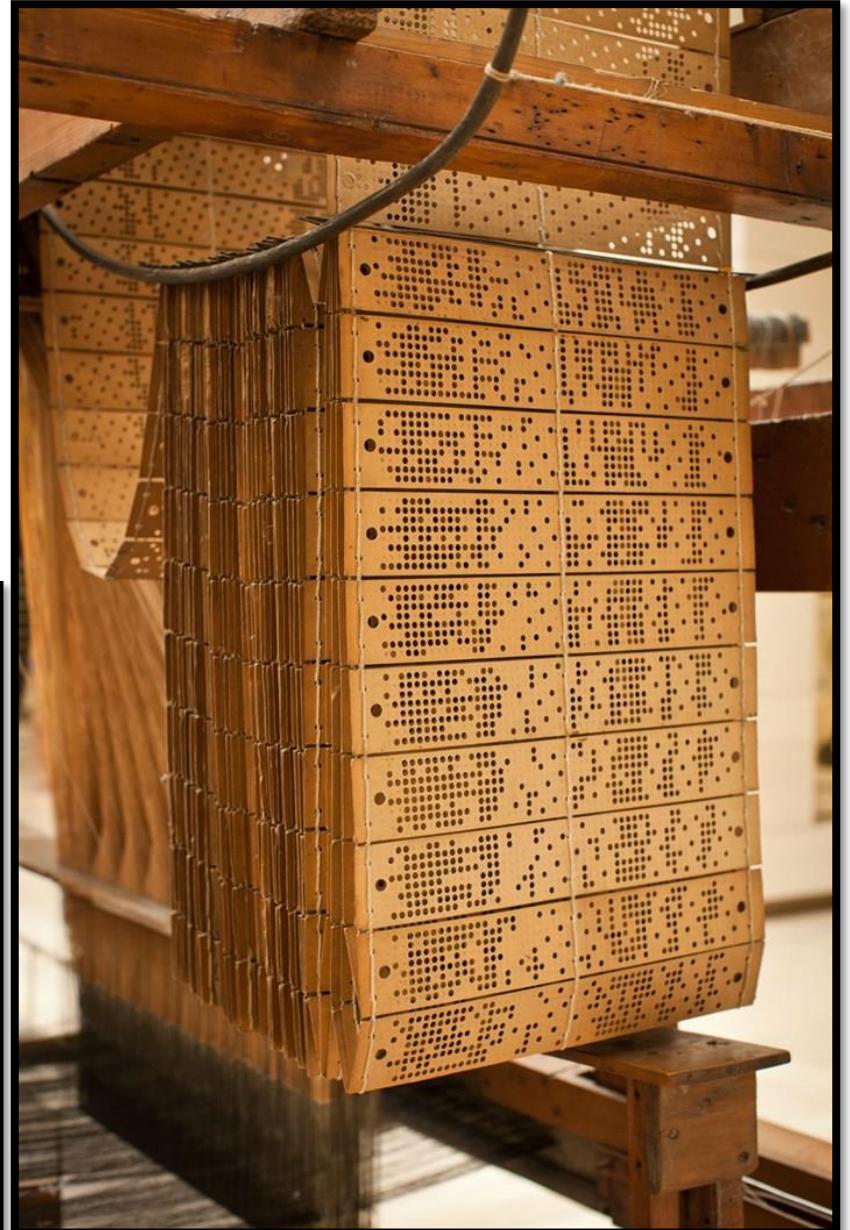
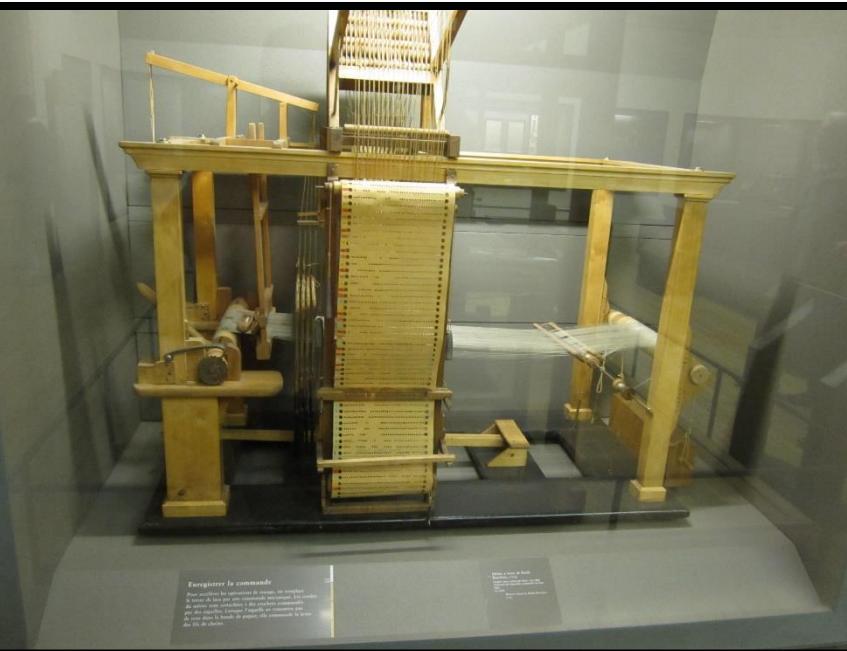
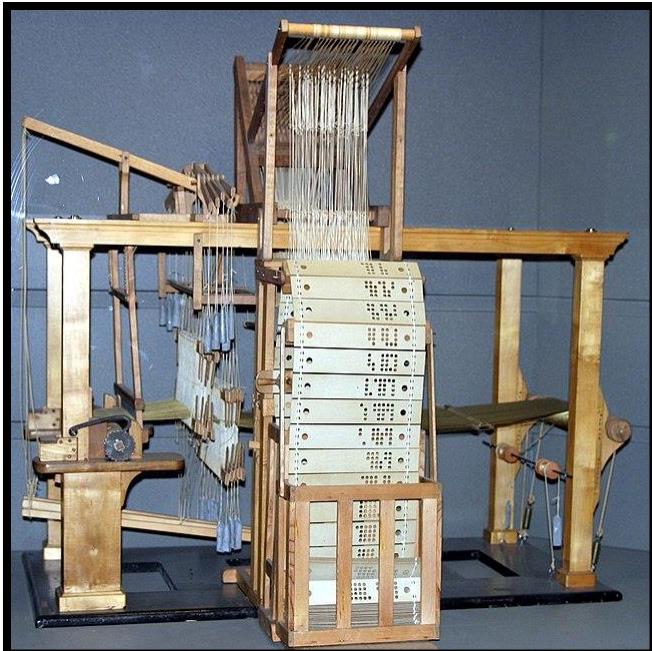
Prima imagine digitală din lume !



Imaginea este doar un exemplu fictiv!

Prima placă grafică (II) - 1745

- Gaură - 1
- Lipsă - 0



Pierre Jaquet-Droz



Roboti mecanici cu memorie (roboti - 1774)



The writer (1774)

Roboti mecanici cu memorie (roboti - 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.



Calculatoare mecanice (uz general)

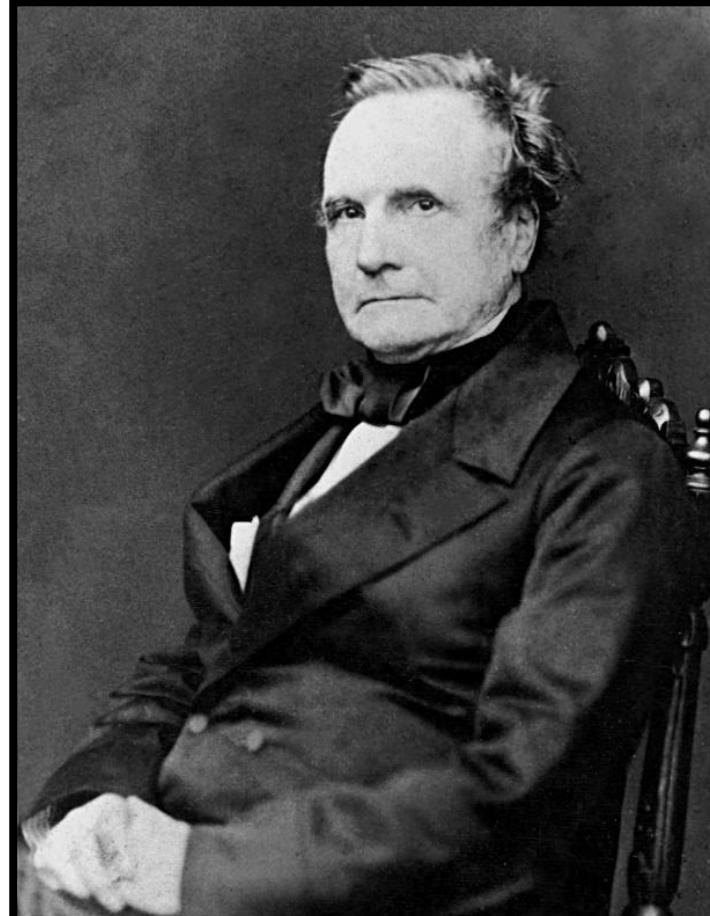
Sfarsitul revolutiei
industriale

Charles Babbage;
“Motorul Analitic”
1830

Dupa
106 de ani

Konrad Zuse; Z1
1936

Calculatorul theoretic “Motorul Analitic” - 1830



Calculatorul Z1 -1936



Charles Babbage (hardware)
Ada Byron (programmer)

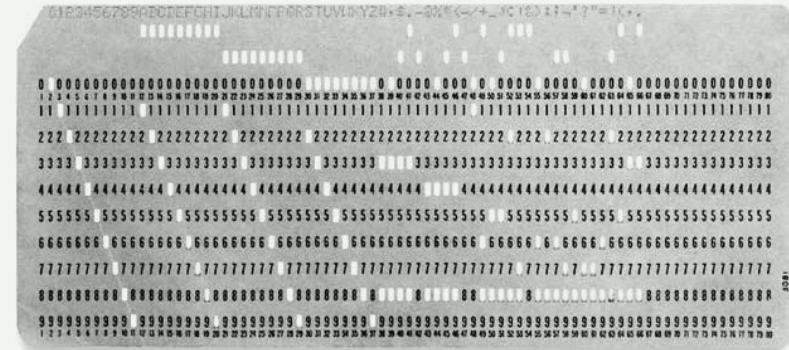
Konrad Zuse

Calculatoare electro-mecanice

Calculatorul Z3 -1941; 5 ani mai târziu...



Konrad Zuse



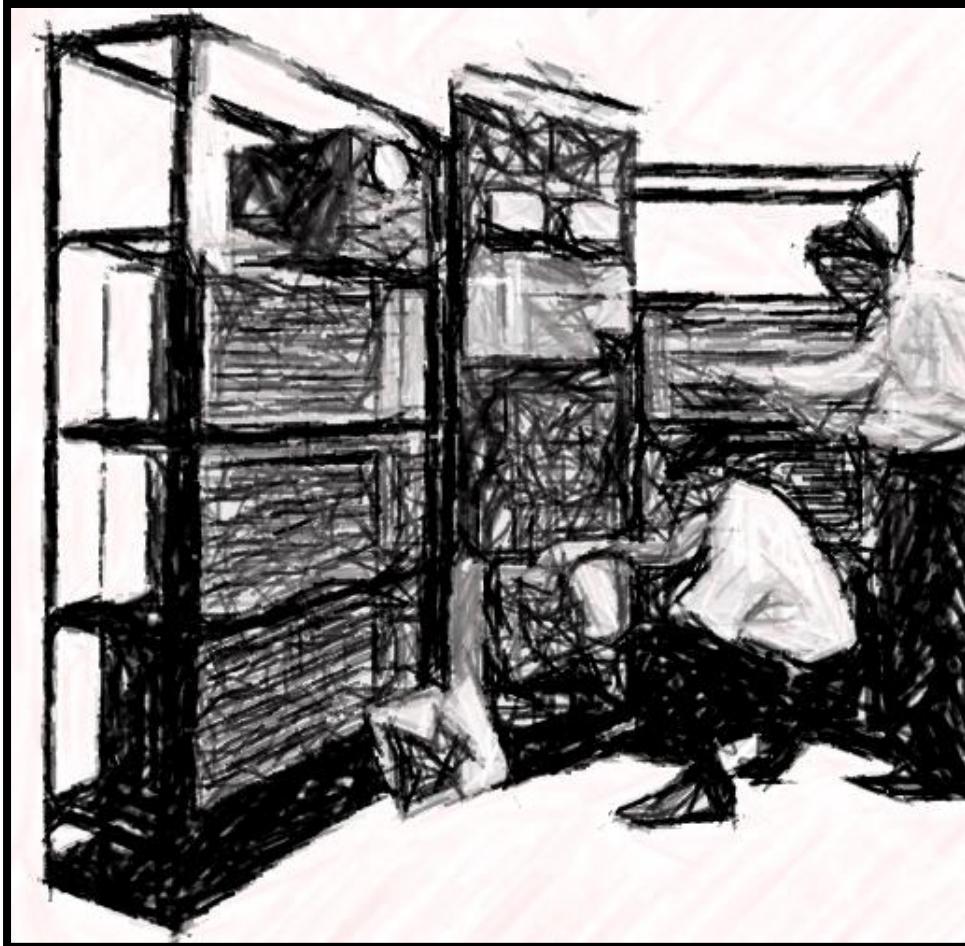
Releu electro-mecanic

Calculatoare electronice

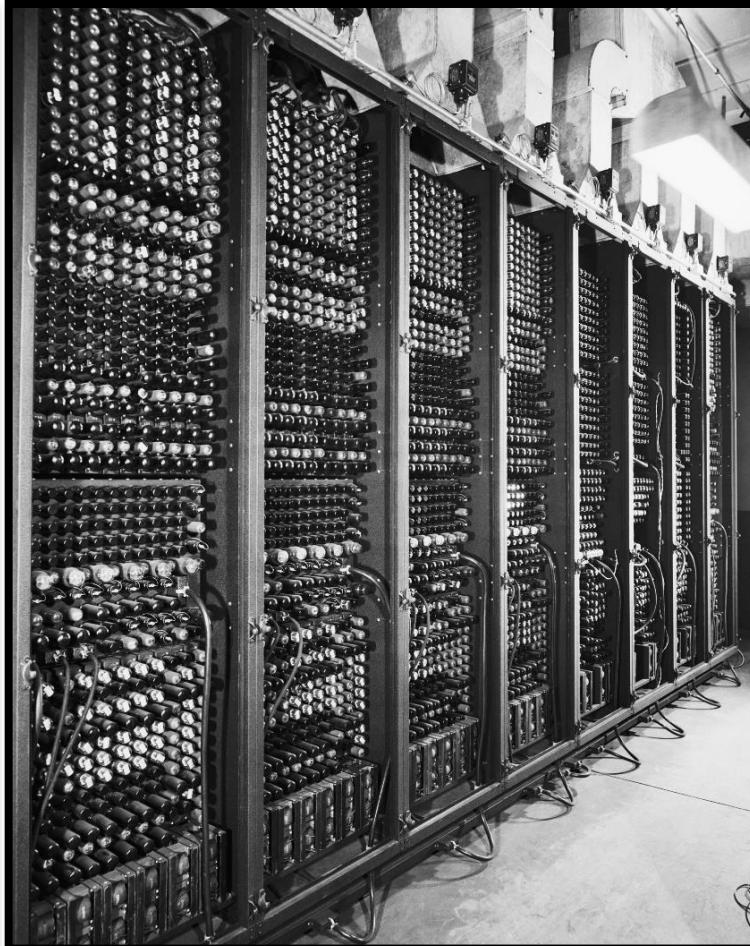
TRADIC – 1950 (pe 800 tranzistoare)



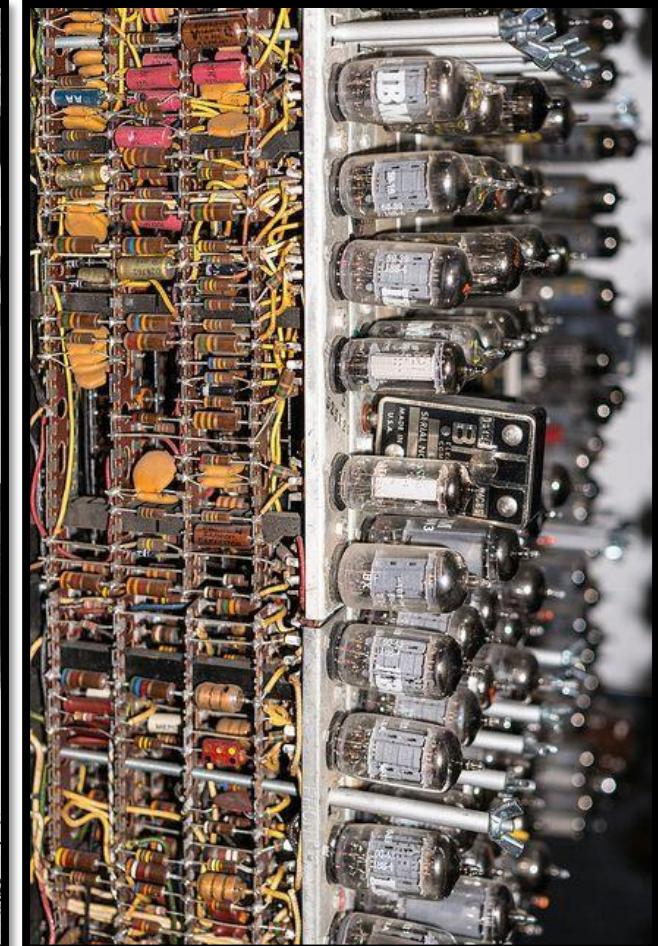
ENIAC – 1945 (pe 17k lampi)



(Transistorized Airborne Digital Computer)



(Electronic Numerical Integrator and Computer)



Calculatoare electronice (piese discrete)



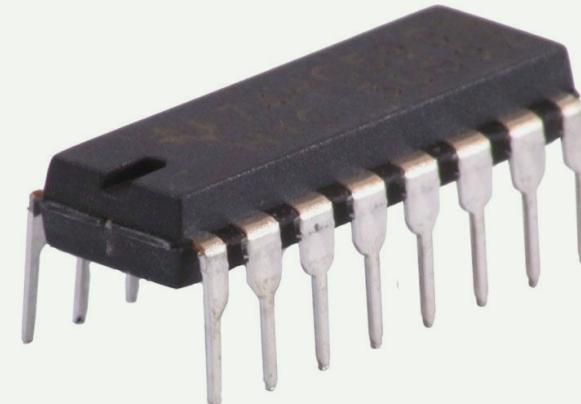
Releul
1835



Tuburi vidate
1907



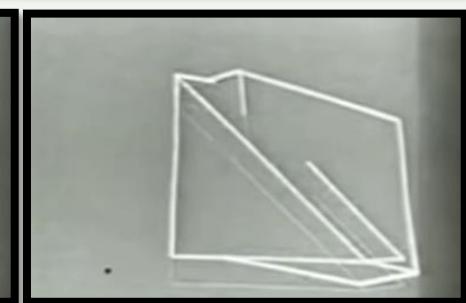
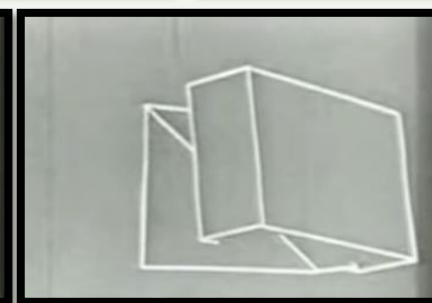
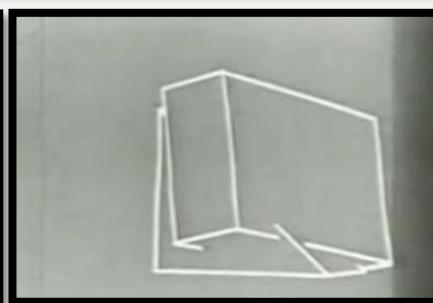
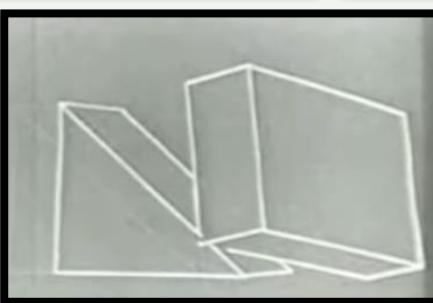
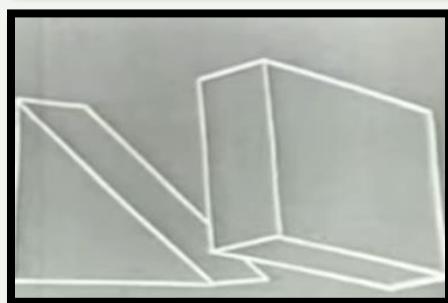
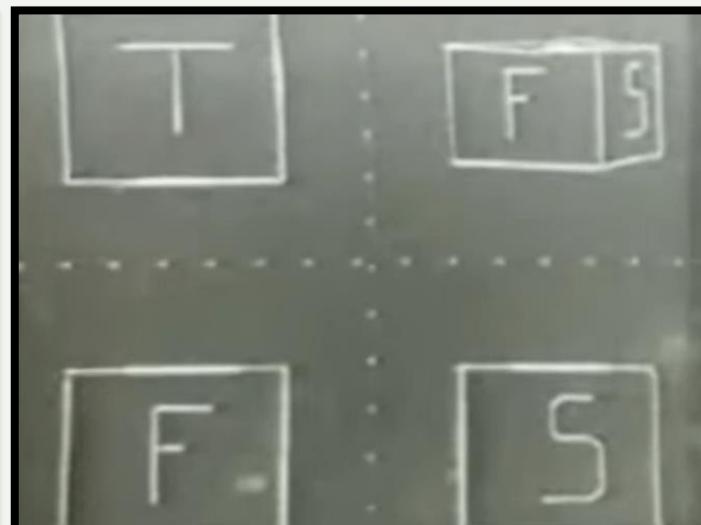
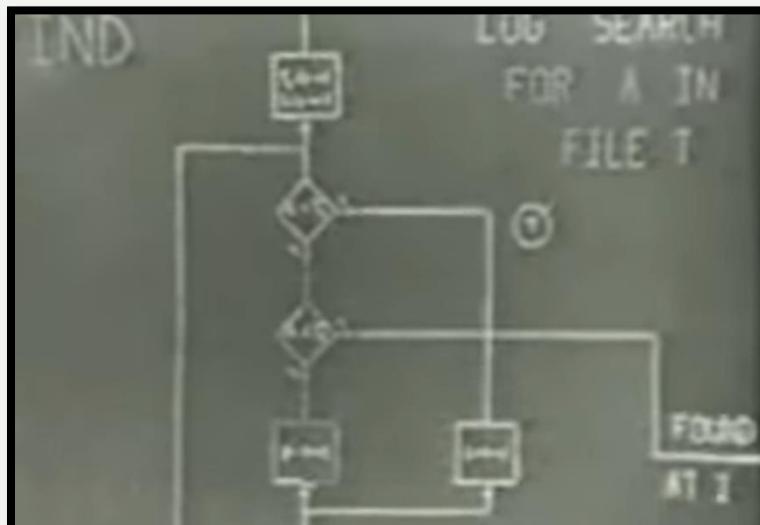
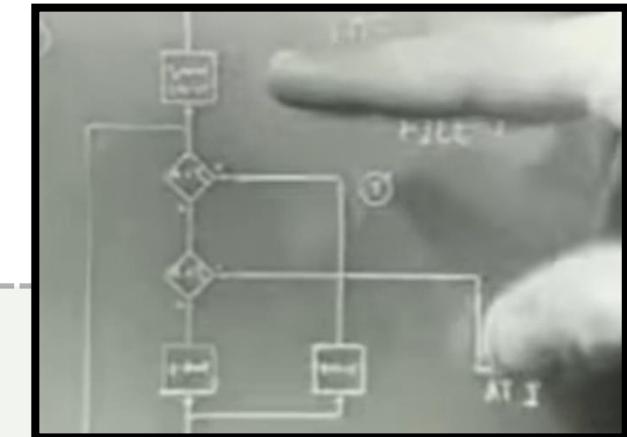
Tranzistori
1947



Circuit Integrat
1963

Prima interfata grafica (GUI)

- 1962 (diagrame, obiecte 3D ...)



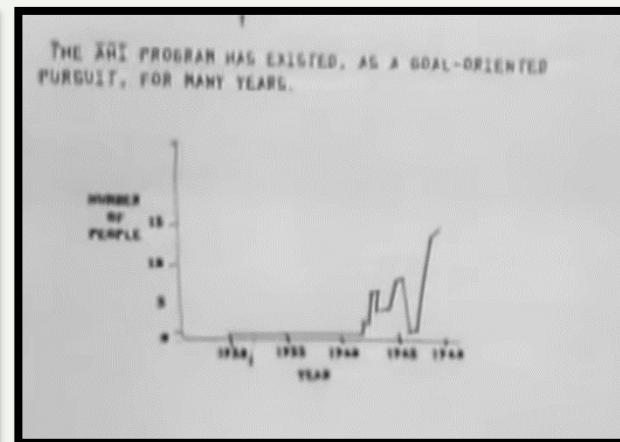
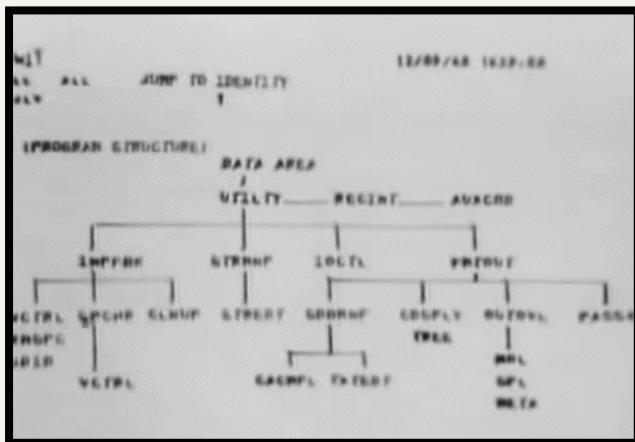
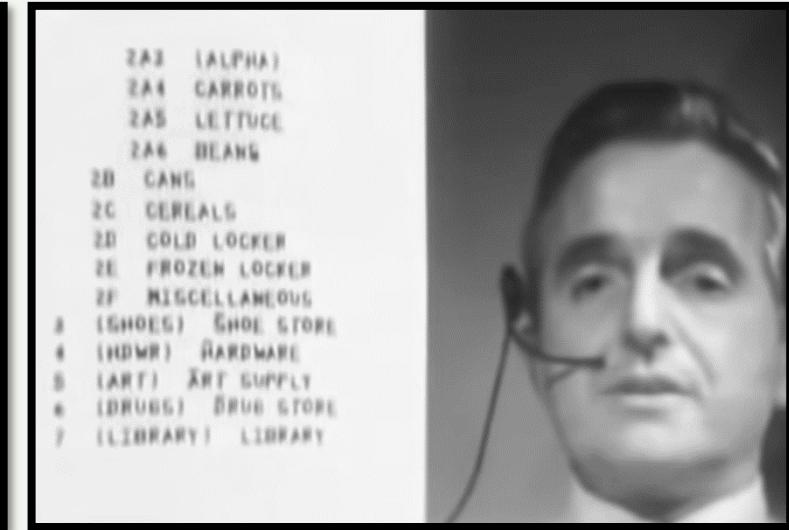
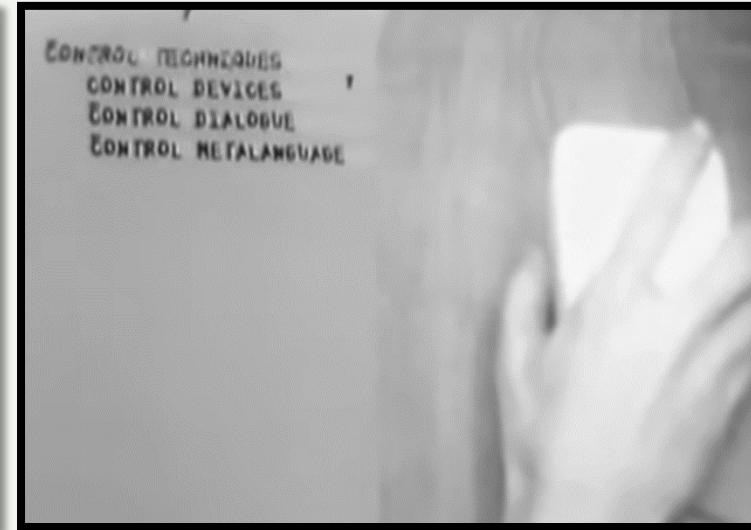
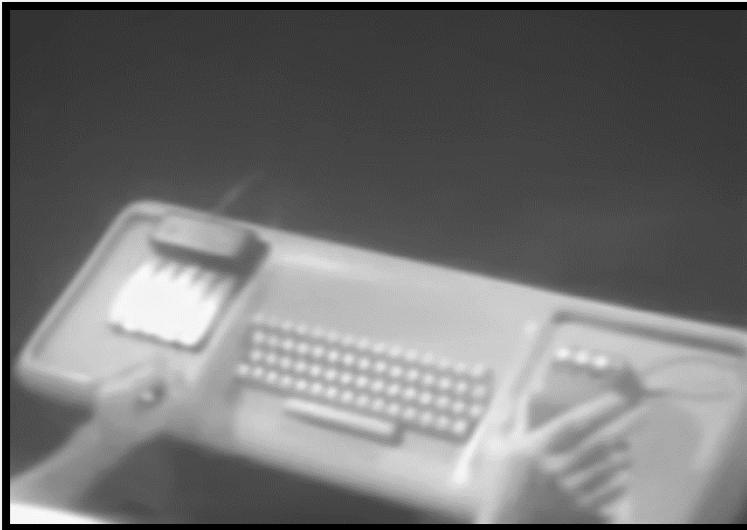
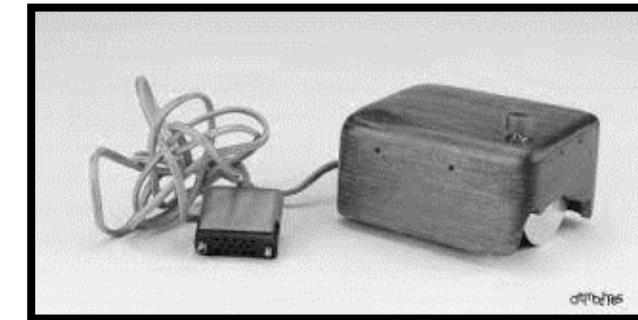
940 SDS

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 extinsă 255 caractere)*

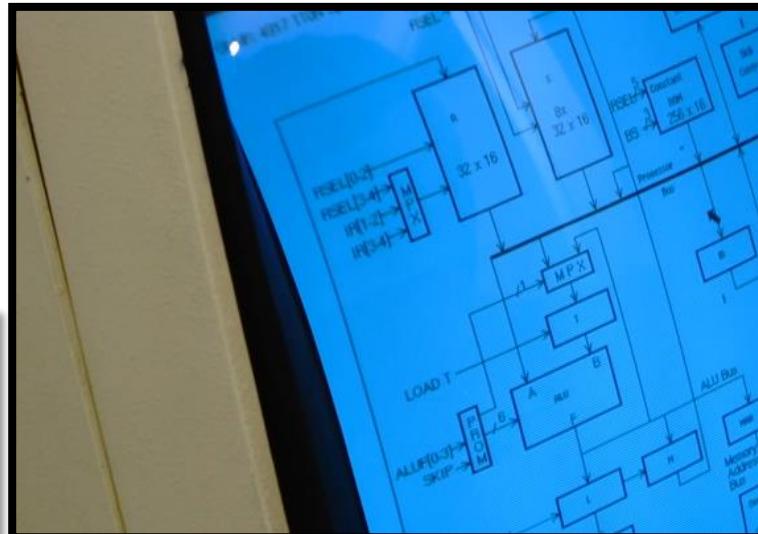
Poziția tastelor pe tastaturile moderne?



Ce reprezintă ASCII?

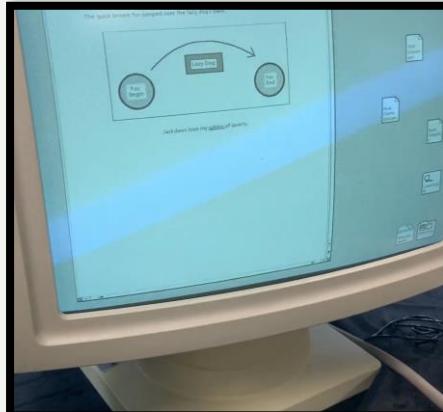
Xerox Alto

1973



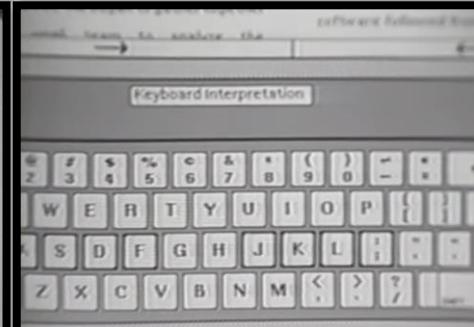
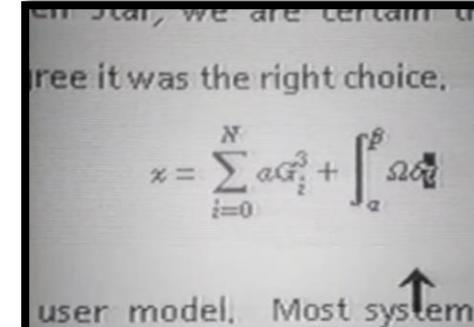
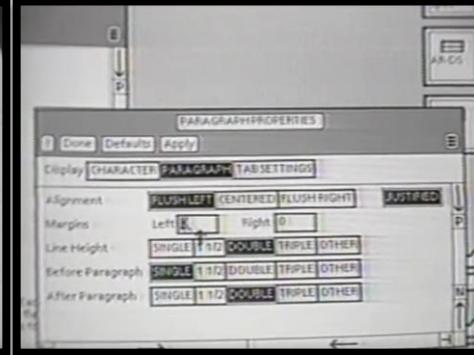
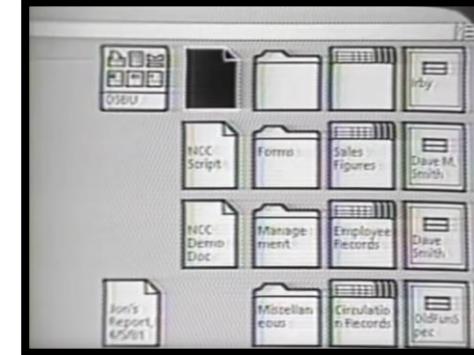
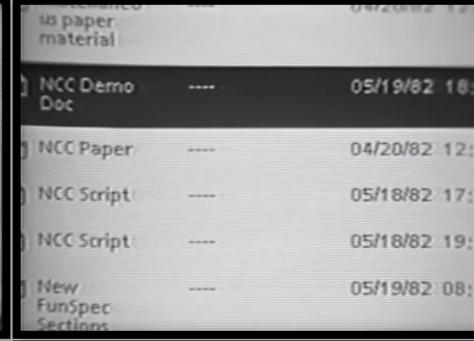
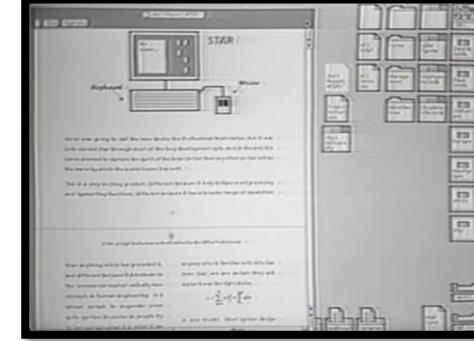
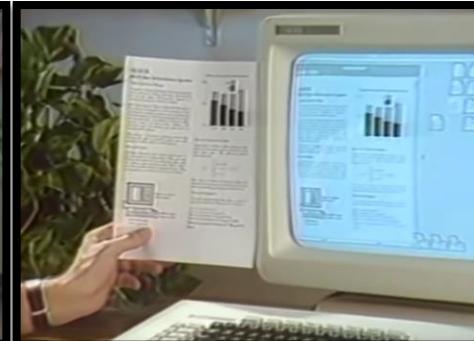
Xerox Star 8010 Computer

1981

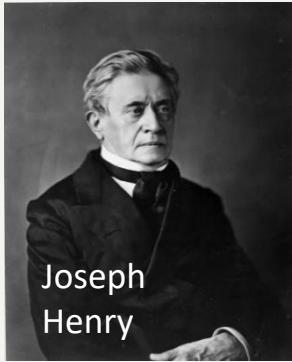


Xerox Star OS
16-bit
8Mhz

Ce observam?



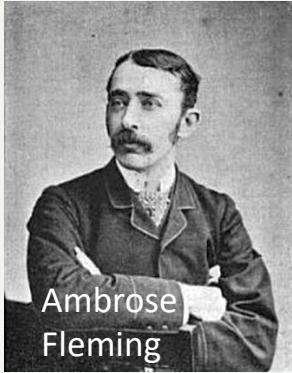
Recapitulare ! De la releu la tranzistor !



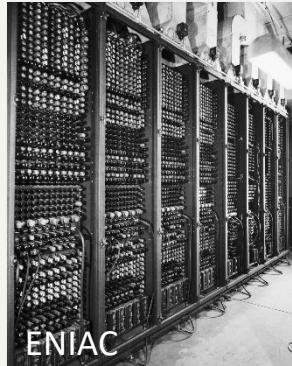
Joseph
Henry



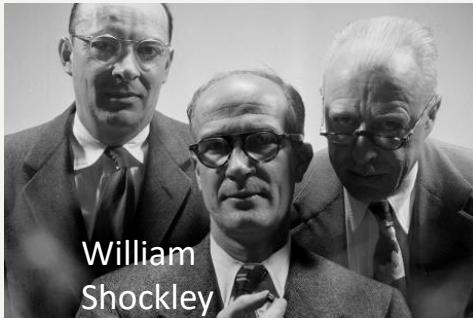
z3



Ambrose
Fleming



ENIAC



William
Shockley



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

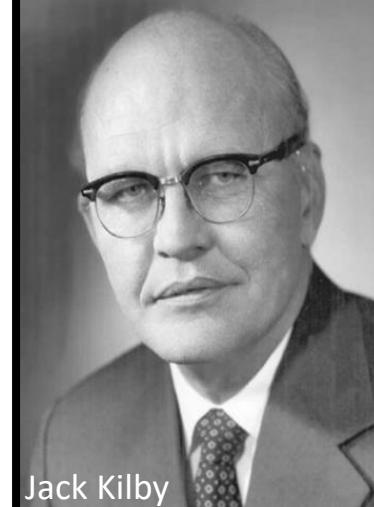
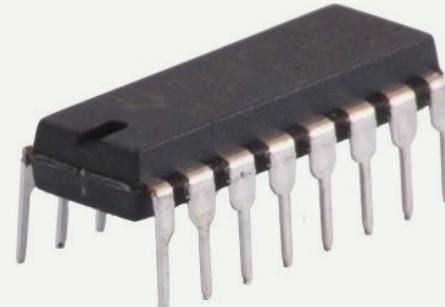
Recapitulare ! Era semiconducatorilor !

Descoperirea efectului de tranzistor

Compactarea in Circuite Integrate (CI)

Primele calculatoare desktop

William Shockley



Jack Kilby



foto-litografie
IC modern
Robert Noyce



Xerox Alto

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

1840

Babbage



1830

1873



1936



1941



1945



1954



1963



1968



1981



First Antivirus

Astăzi



1835

Codul Morse (1837)
si telegraful (1844)



1907

Konrad Zuse
z1

Konrad Zuse
z3

ENIAC

TRADIC

Primul GUI

Douglas Engelbart
940 SDS

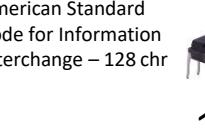
Xerox Star

First Antivirus

1963
ASCII



1947



1963



1972

Xerox Alto

Apariția treptată a
aplicațiilor malware
din 1971

99% din toate fenomenele fizice au fost descoperite

WWI

(1914-1918)

WWII

(1939-1944)

1972



Xerox Alto

1981



Xerox Star

*File Virus;
MS-DOS;

Cascade
1987

.exe
(resident)

*Backdoor;
VAX/VMS
OS;

Vienna
1987

.com
(non-resident)

WANK
1989

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

1971
Creeper

*Worm;
TENEX OS;
ARPANET

Mainframe

1975
Animal

*Trojan;
UNIVAC 1100
OS

1982
Elk Cloner

*Boot Virus;
Apple II OS

1986
Brain

*Resident
Boot Virus;
MS-DOS

1987
Stoned

Boot Virus;
MS-DOS

1988
Morris

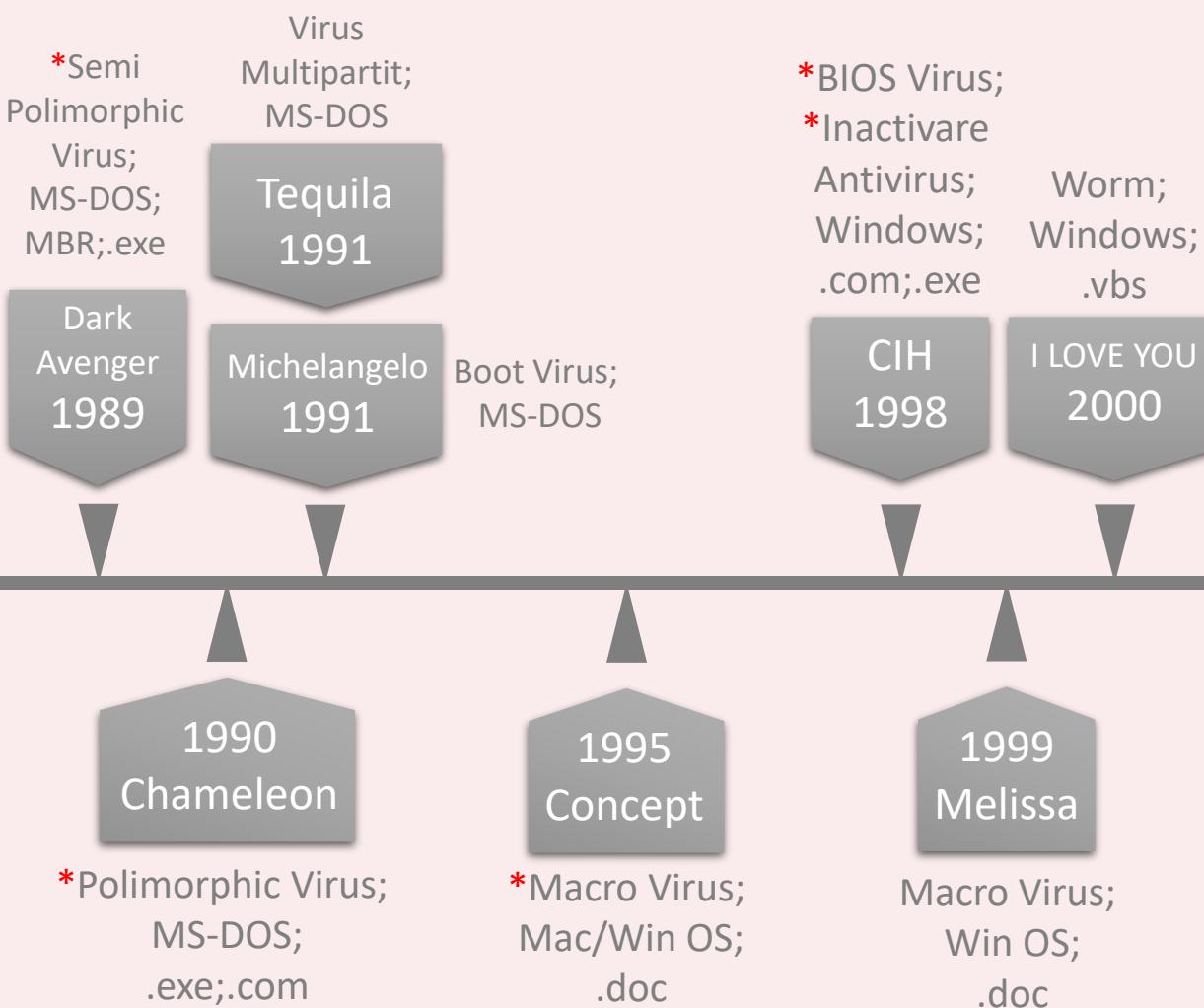
Worm;
UNIX;
*(resident
RAM)

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)

Explorarea evoluției malware-ului (I)

1970 - 1990



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 dezaktivat o soluție antivirus (Norton AV; suprascrierea fișierelor)

Calculatoare personale (PC)
 Mainframes (calculator central de mare putere)

Explorarea evoluției malware-ului (II)

1990 - 2000

Worm;
Windows;
(resident RAM)

Code
Red
2001

Worm;
Windows;
(resident RAM)

Blaster
2003

Worm;
Windows;
(fis. bin)

Conficker
2008

Trojan;
Windows;
.*

Zbot
2010

2001
Nimda

2004
Mydoom

2010
Stuxnet

Worm;
Win OS;
.doc

*Virus/Worm;
Windows;
email
.eml;.exe

Virus/Worm;
Windows;
email
.exe;.zip;.scr

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

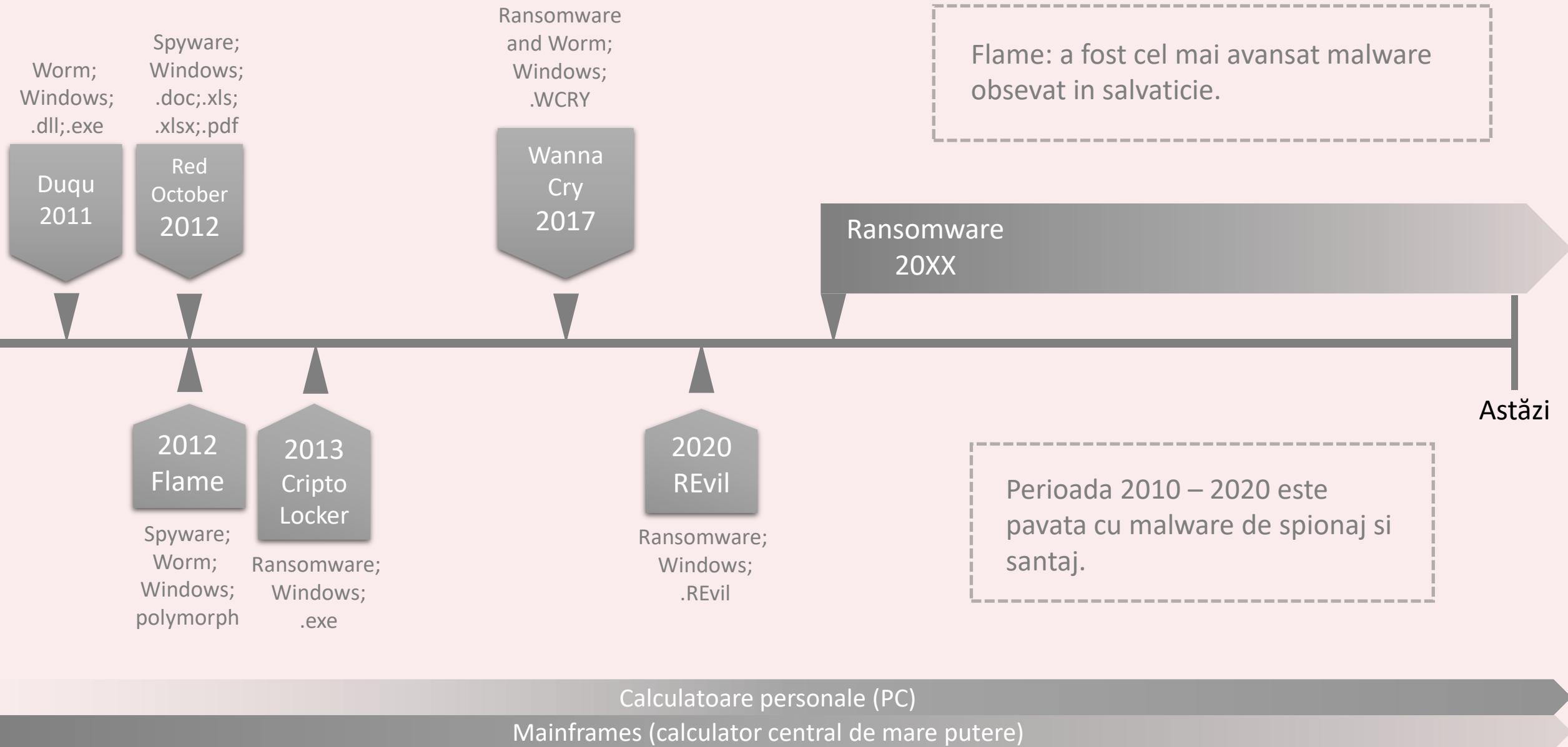
Nimda a fost unul dintre primele virusuri care a combinat caracteristicile unui virus cu cele ale unui vierme.

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

Calculatoare personale (PC)
Mainframes (calculator central de mare putere)

Explorarea evoluției malware-ului (III)

2000 - 2010



Explorarea evoluției malware-ului (VI)

Tipuri de malware/Decada

Distributia aproximativa:

Anii 1970

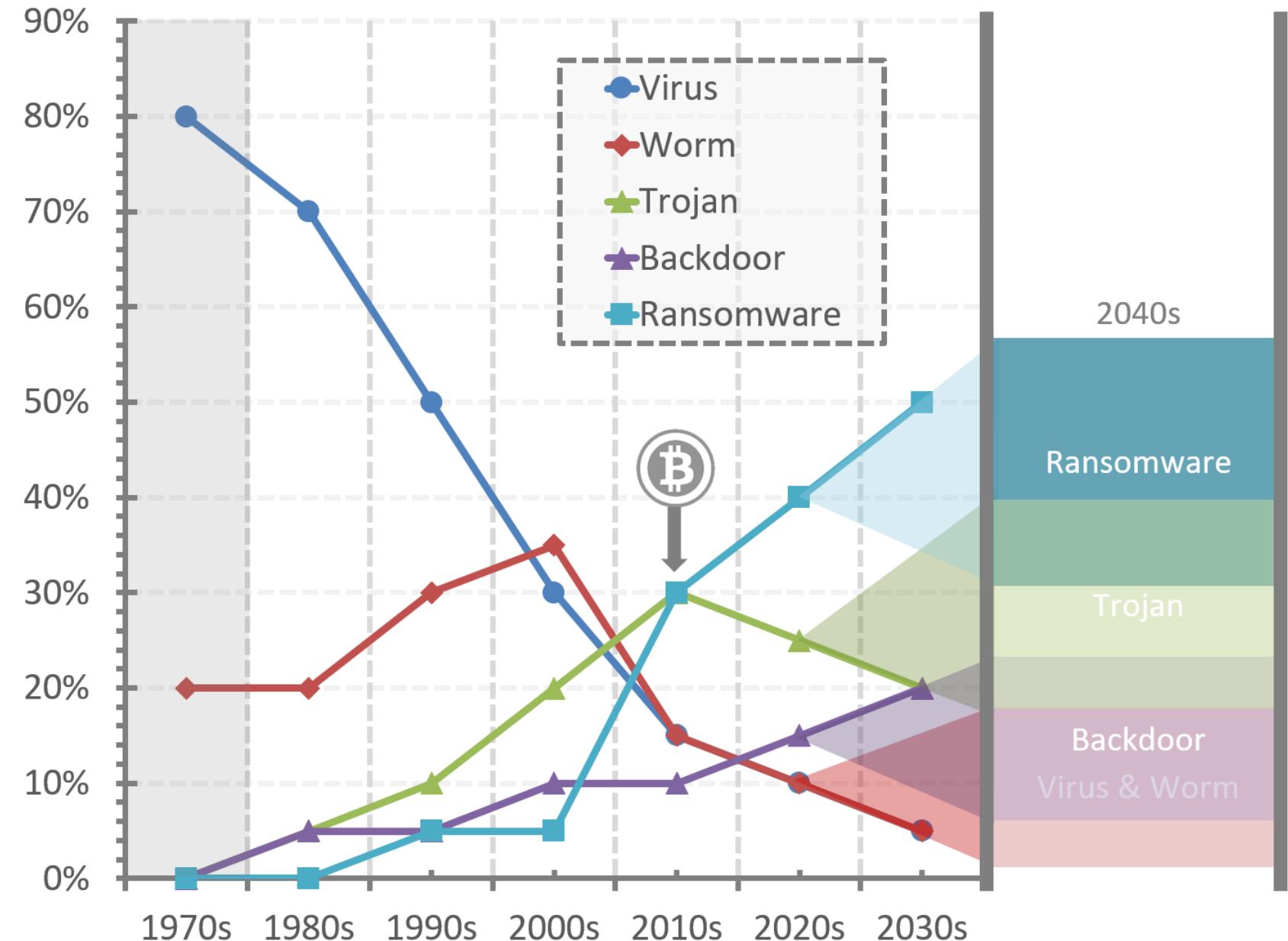
Virus: 80%
(Discuții mai mult teoretice și dezvoltări timpurii)

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

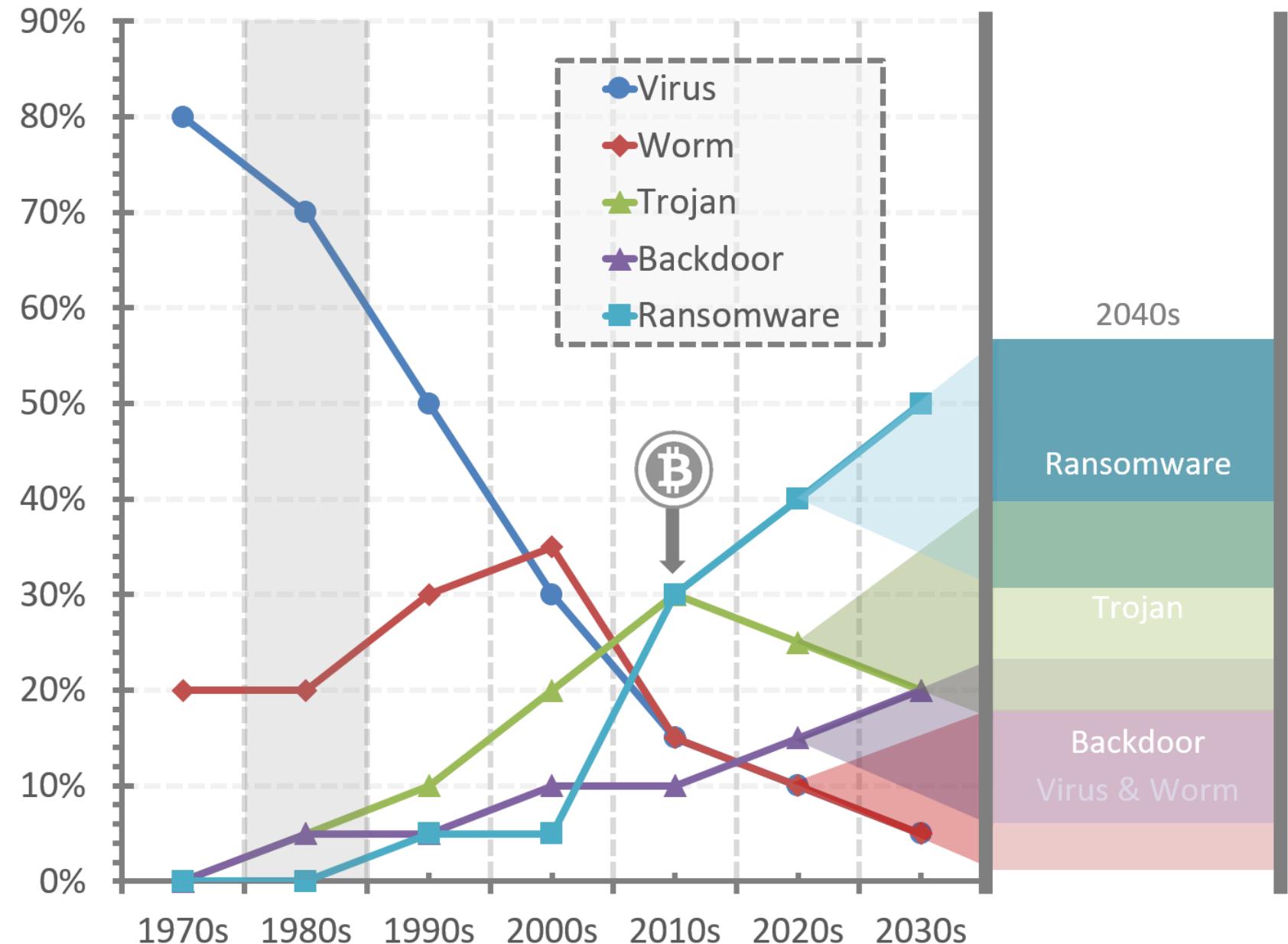
Virus: 70%
(Creșterea virusilor de PC)

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

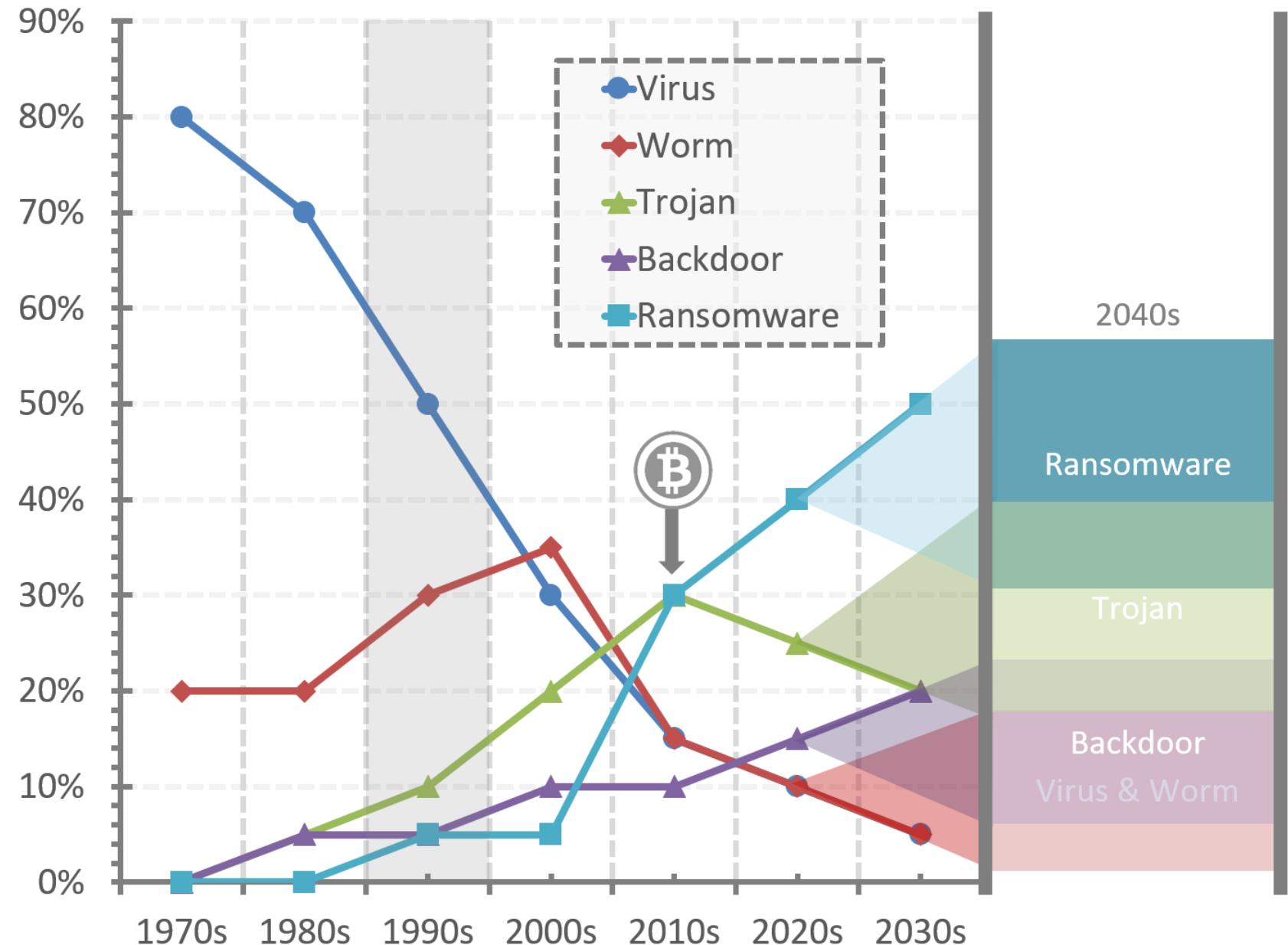
Virus: 50%
(Proliferare larg răspândită)

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:

Anii 2000

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

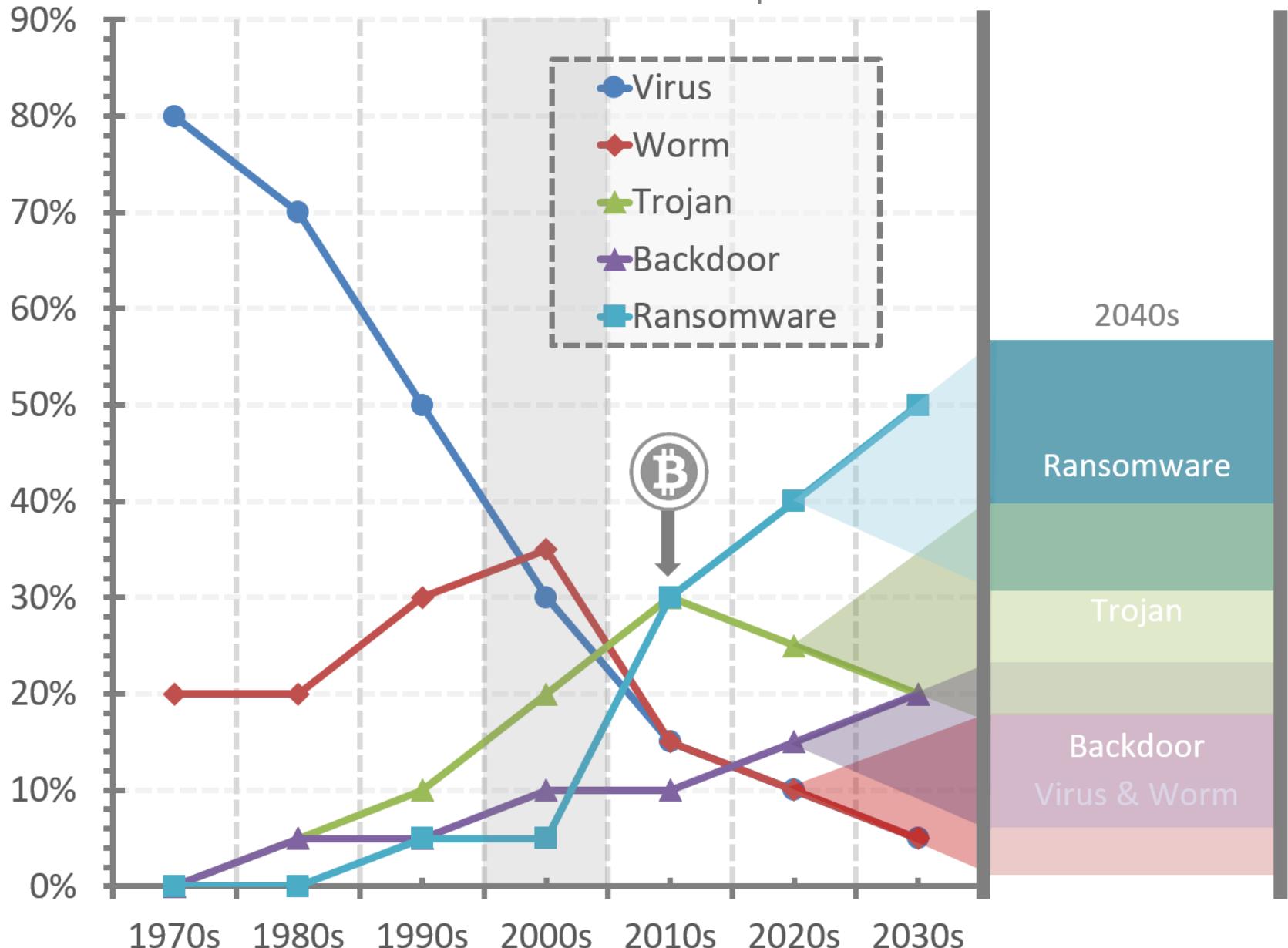
Worm: 35%
(Vârful activităților worm
cu focare globale majore)

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

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

Ransomware: 5%
(Emergența
ransomware-ului modern)

Conturi bancare - identitate reală:
- Cumpărare produse – la adresa – vânzare ulterioară.
- Cont bancar real - persoana frontală – ridicare bani.



Tipuri de malware/Decada

Distributia aproximativa:

Anii 2010

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

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

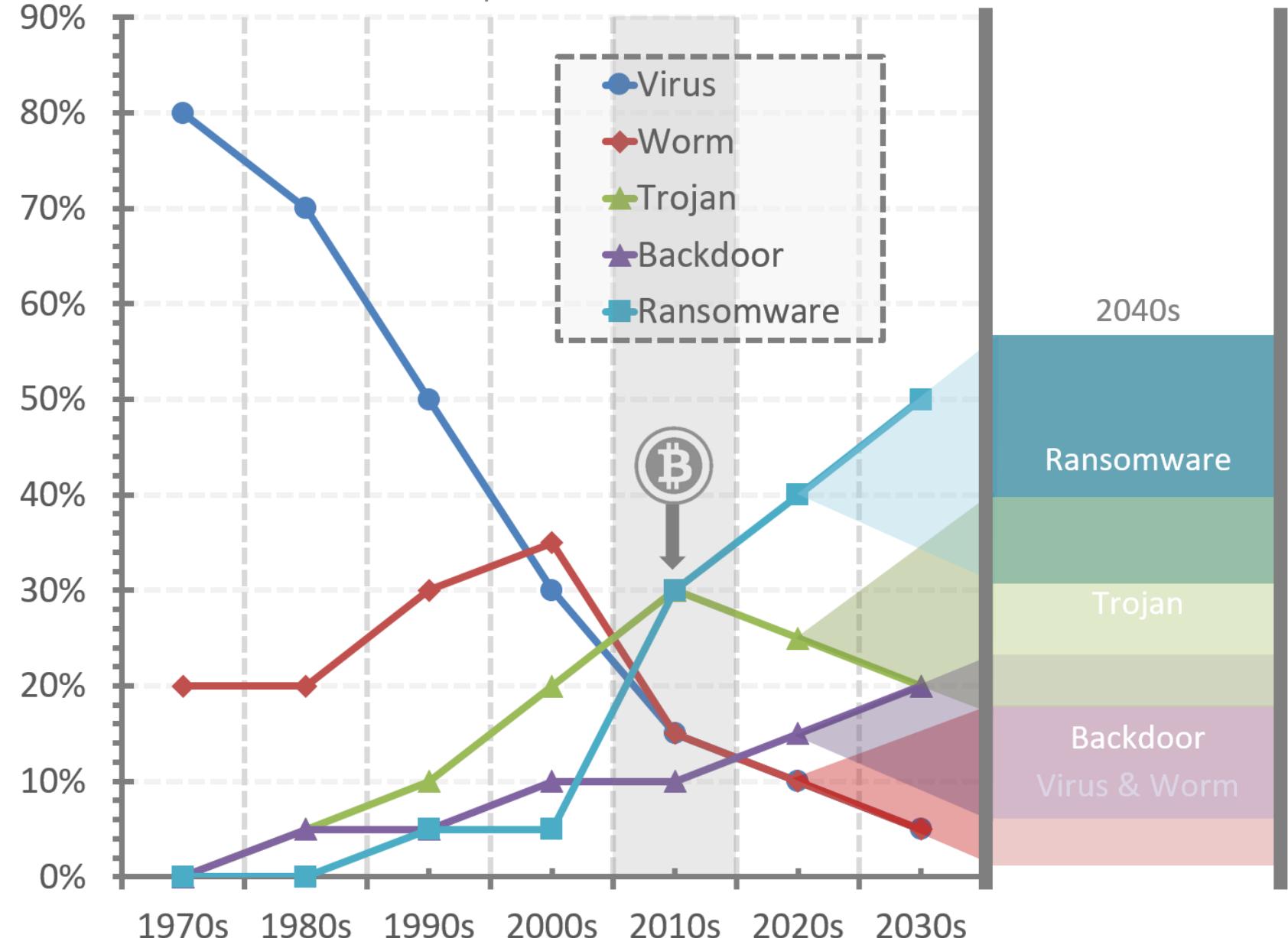
Trojan: 30%
(Semnificativ sub forma APT-urilor și troienilor bancari)

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

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

Apar criptomonezi:

- Incontrolabile – identitate necunoscuta.
- Independent de sistemul bancar.



Tipuri de malware/Decada

Distributia aproximativa:

Anii 2020

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

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

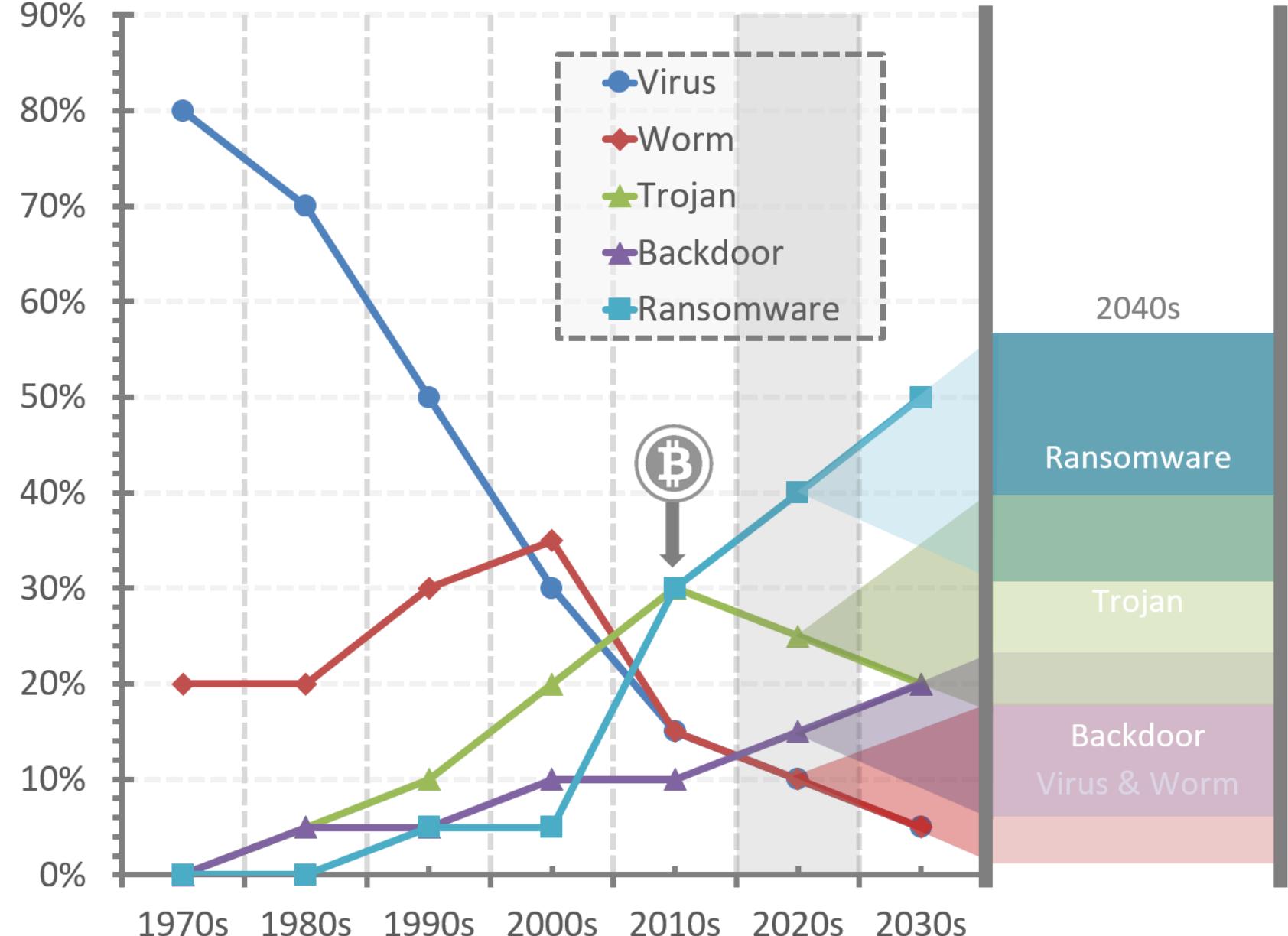
Trojan: 25%
(Continuă să fie important,
mai ales în atacuri țintite)

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

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

Adaptarea la criptomonezi:

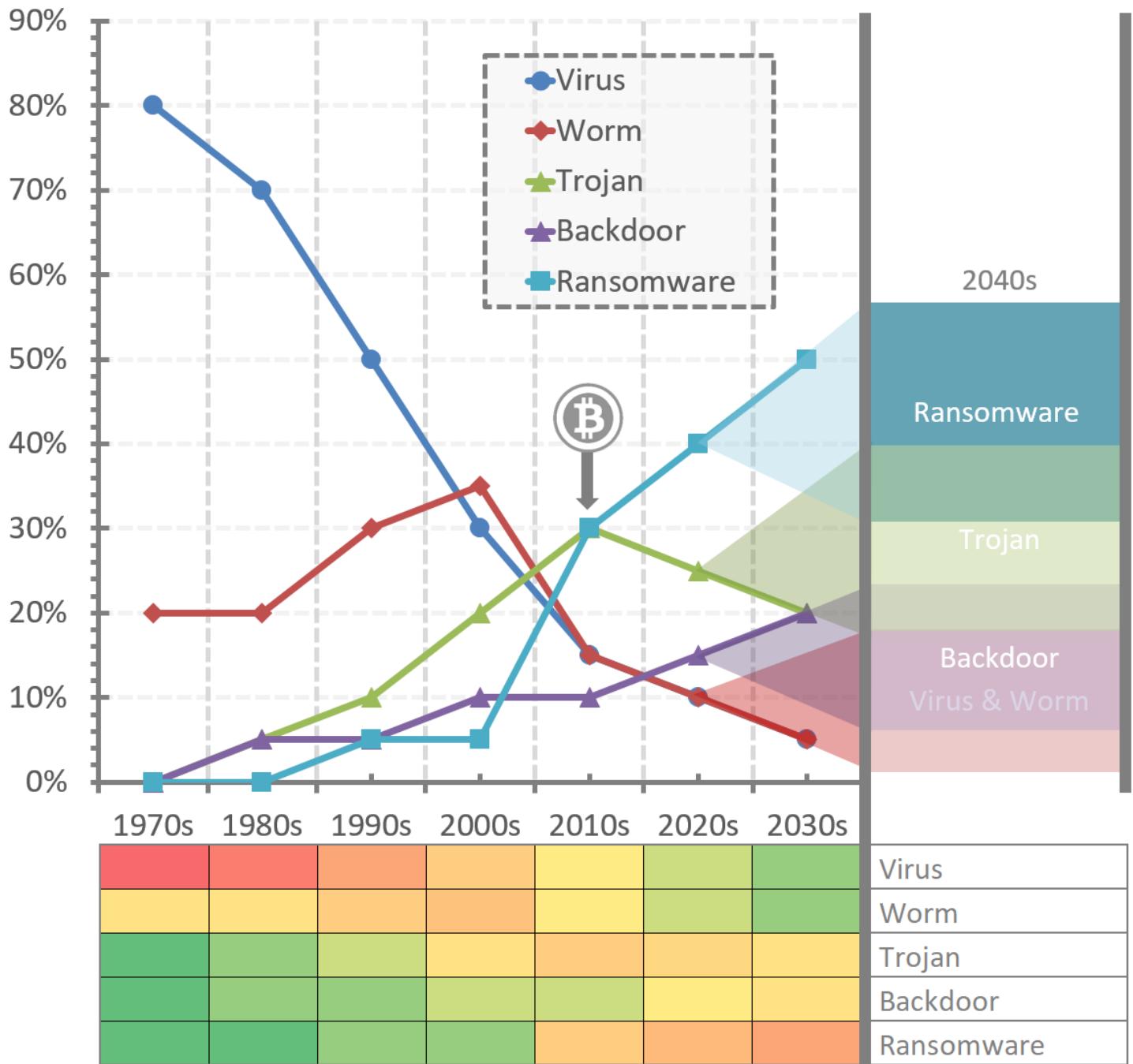
- Reutilizarea malware pentru șantaj.
- Ascendent doar Ransomware și Backdoor.



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.



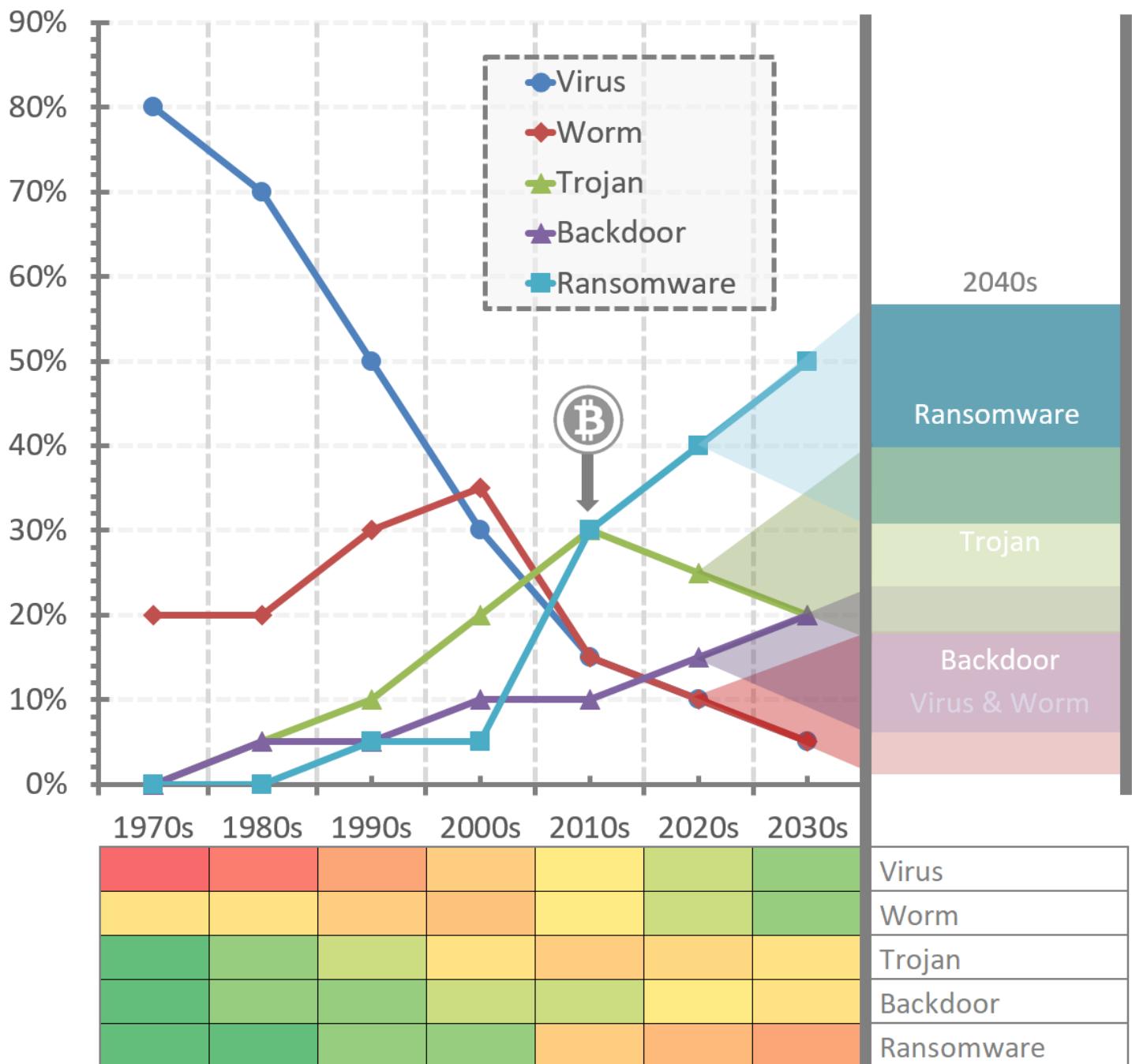
Tipuri de malware/Decada

Distributia aproximativa:

- De ce nu mai observam virusi?
- OS mai vechi au fost eliminate treptat (procese izolate, restrictii).
- Nimeni nu trimit 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 încide ușor o potentială vulnerabilitate.



c.1.3

EVOLUȚIA SOLUȚIILOR DE SECURITATE

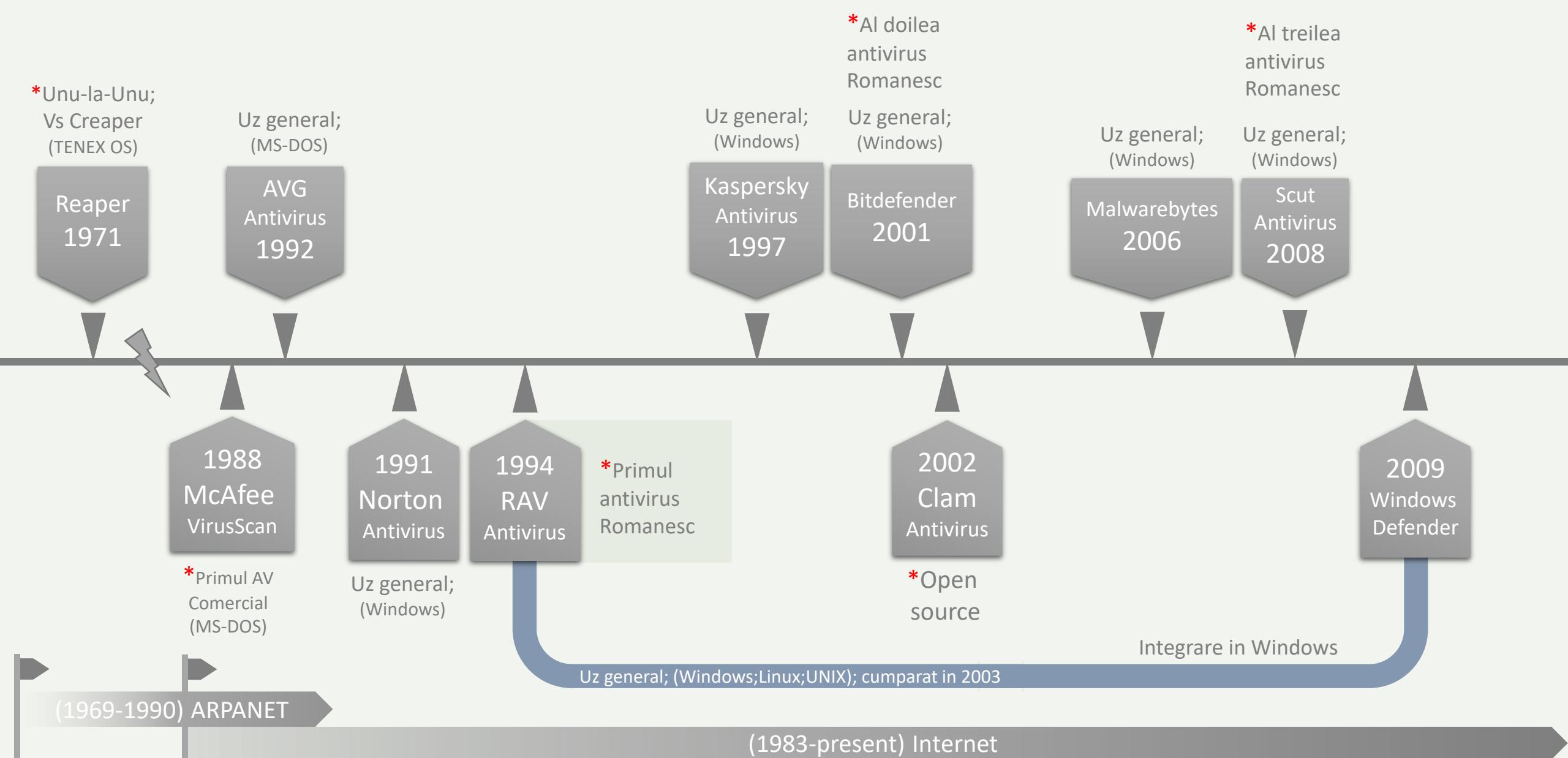


Biologie vs. masini artificiale

Sistem imunitar

Malware

Antivirus



Solutii antivirus !

Companiile AV serioase & discriminarea optima.

1970 - 2010



INTERNET ARCHIVE

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

GLOBAL ADVANCED TECHNOLOGY

SCUT ANTI VIRUS

SCUT FAMILY SYSTEM INFORMATION SECURITY

OUS CUSTODIET IPSOS CUSTODES
CONSILIO ET PRUDENTIA

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 vulnerabilities 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

INTERNET ARCHIVE
WayBack Machine

Puțin despre soluția Scut Antivirus



The screenshot displays the main interface of the SCUT Anti Virus software. The top bar includes tabs for "AntiVirus Status", "Firewall Engine", and "Scut World System". The "AntiVirus Status" tab is active, showing metrics like "Colectiv Concience" (100%), "Colectiv Defence" (100%), and "Scut machines online" (100%). The "Firewall Engine Version" is listed as 1.9.0.6. The "Scut World System" tab shows a world map with various status points. A central banner displays the "Scut AntiVirus" logo. The bottom navigation bar includes links for "Anti Virus", "Fire Wallq", "Status", "Report", "Scule", "Optiuni", "Suport", and "Actualizare". A watermark for "INTERNET ARCHIVE WayBack Machine" is visible across the bottom of the interface.

VX Heaven – Importanță băncilor malware!

VX Heavens

Library Collection Sources Engines Constructors Simulators Utilities Links Antivirus Forum

Hosted sites

[eof-project.net](#)

[bi0tic.info](#)

[29a](#)

[Berniee](#)

[Bull Moose](#)

[DCA](#)

[Doomriderz](#)

[IKX](#)

[FAMINE](#)

[herm1t](#)

[hh86](#)

[Positron](#)

[V-Codez](#)

[WarGame](#)

Friendly sites

[FreeThinking](#)

[Scut Anti Virus](#)

[DUSecurity Group](#)

[Your link here?](#)

Viruses don't harm, ignorance does!

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Article 19 of "Universal Declaration of Human Rights"

Welcome to VX Heavens! This site is dedicated to providing information about computer viruses (or virii, as some would prefer) to anyone who is interested in this topic.

This site contains a massive, continuously updated collection of magazines, virus samples, virus sources, polymorphic engines, virus generators, virus writing tutorials, articles, books, news archives etc. Even the viruses for the platforms you've never heard of. We also offer free hosting for virus authors and groups.

Some of you might reasonably say that it is illegal to offer such content on the net. Or that this information can be misused by "malicious people". I only want to ask that person: *"Is ignorance a defence?"*

webmaster@vx.netlux.org 

You can help us improve the site by [uploading new stuff](#), [making a donation](#), posting our link to your site, blog or forum, or [leaving a comment](#). Thank you!

What's new? (January 2010)

28 + LIB/EN: Int13h "The short monologue of virus Wendell from his small 120 megabytes world" 

27 + LIB/EN: Adam Reynolds "I.T. IN PRACTICE: Computer viruses" 

27 + LIB/EN: Eugene Spafford "Computer Viruses and Ethics" 

26 + LIB/EN: Star0 "C to assembly, language point of view" 

VX Heaven

Library Collection Sources Engines Constructors Simulators Utilities Links [Donate](#) [Forum](#)

Hosted sites

[29a, hell knights crew, Berniee, Bull Moose, DCA, Doomriderz, herm1t, IKX, Positron, RRLF, SPTH](#)

Friendly sites

[Scut Anti Virus](#)

[Virus News](#)

[Virus Collection](#)

[Your link here?](#)

Viruses don't harm, ignorance does!

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Article 19 of "Universal Declaration of Human Rights"

Welcome to VX Heaven! This site is dedicated to providing information about computer viruses (or virii, as some would prefer) to anyone who is interested in this topic.

This site contains a massive, continuously updated collection of magazines, virus samples, virus sources, polymorphic engines, virus generators, virus writing tutorials, articles, books, news archives etc. Even the viruses for the platforms you've never heard of. We also offer free hosting for virus authors and groups.

Some of you might reasonably say that it is illegal to offer such content on the net. Or that this information can be misused by "malicious people". I only want to ask that person: *"Is ignorance a defence?"*

You can help us improve the site by [uploading new stuff](#), [making a donation](#), posting our link to your site, blog or forum, or [leaving a comment](#). Thank you!

webmaster@vxheaven.org

STOP RUSSIAN AGGRESSION AGAINST UKRAINE!

What's new? (March 2016)

No news is a good news :-)

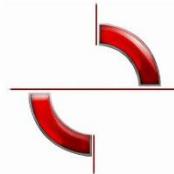
Latest discussions on forum:

CaptainTech in [Can a virus actually damage PC hardware?](#) (2016-03-28 23:14:04)

Xylitol in <http://www.9supplements.org/1k-daily-profit/> (2016-03-28 22:43:51)

alcopaul in [\[Q\] Meaning of numbers in the virus alias](#) (2016-03-28 21:36:14)

siek in <http://www.9supplements.org/1k-daily-profit/> (2016-03-28 21:02:13)



Automatizare extragere de semnaturi

Scut AntiVirus

In acest modul se introduc automat doar fisierile virus curate, semnaturile luate din fisierile infectate se editeaza manual !

Scut antivirus

Scrie noua baza de semnaturi !

Director banca malware
Cale: C:\Users\Paul\Desktop\...
Masca: *.*

Cautare opțiuni

Atribute fisiere:

- Normal
- Arhivat
- Ascuns
- Către numai
- System

Optiuni:

- Pattern Matching
- Cautare in sub-direcțoare
- Sortarea fisiere (A-Z)
- Reimpresatare ListView
- Use Extended Mode Scan

Filtrare date/dimensiune:

Dupa data: Modified
De la: 9/23/2023
la: 12/23/2023
Dim fisier: Any Size

Scan
1255

File
Trojan-Game Thief.Win32.M...
Trojan-Game Thief.Win32.M...
Trojan-Game Thief.Win32.M...
Trojan-Game Thief.Win32.M...
Trojan-Game Thief.Win32.M...
Trojan-Game Thief.Win32.M...

Geneza semnaturi ... Stop

DB virusi!

Operati

- [Deschide DB >](#)
- [Salveaza manual](#)
- [Update manual](#)
- [Sterge inregistrarea](#)
- [Sterge DB-ul](#)

Semnaturi

FieldCount > 4	Lungime semnatura	
Sig 1	é, mcN-mcN-mcNÖqoNÖmcN.qmNn	50
Sig 2		50
Sig 3	50 Backdoor.Win32.Aimbot.dz	50
Info	Backdoor.Win32.Aimbot.dz	50

<< < > >>

Position 0

Găsește semnatura sau nume malware !

Backdoor.Win32.Aimbot.dz

Găsește inregistrare ! Camp -1 Start: |

Coincidente

Text :

```
éLC²LJ'Íló[0-1AEó-ÚúØ‰AIP^||zCULé
```

Ideal : 2.33% Kappa

Rezultate :

Offset : IC :	Coincidente :
1	0%
2	0%
3	0%
4	0%
5	0%
6	0%
7	0%
8	4.76%
9	0%
10	0%
11	0%
12	0%
13	0%
14	0%
15	0%
16	0%
17	0%
18	3.12%

BINAR - Virusi din care nu s-a extras nimic: [17]

C:\Users\Paul\Desktop\banca\vir\Backdoor.V...
C:\Users\Paul\Desktop\banca\vir\Exploit.Linu...
C:\Users\Paul\Desktop\banca\vir\Exploit.Wind...
C:\Users\Paul\Desktop\banca\vir\Rootkit.Win...
C:\Users\Paul\Desktop\banca\vir\Trojan-Click...
C:\Users\Paul\Desktop\banca\vir\Trojan-Dow...
C:\Users\Paul\Desktop\banca\vir\Trojan-Dow...

BINAR - Semnatura mai mica de 20: [17]

C:\Users\Paul\Desktop\banca\vir\Backdoor.V...
C:\Users\Paul\Desktop\banca\vir\Backdoor.V...
C:\Users\Paul\Desktop\banca\vir\Backdoor.V...
C:\Users\Paul\Desktop\banca\vir\Backdoor.V...
C:\Users\Paul\Desktop\banca\vir\EmailWorm...
C:\Users\Paul\Desktop\banca\vir\Exploit.Linu...
C:\Users\Paul\Desktop\banca\vir\Exploit.Wind...
C:\Users\Paul\Desktop\banca\vir\HackTool.V...
C:\Users\Paul\Desktop\banca\vir\Rootkit.Lin...

Coincidenta in jur de : 0.44%

Distanța fata de sig:150 Admins coincidenta: 50 Admins nr caractere: 10

Creaza DB si INDEX sorteaza

RecordCount > 16

DataBase opened...

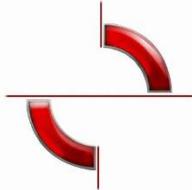
The screenshot shows the Semnaturi interface with the following details:

- Director banca malware:** C:\Users\Paul\Desktop\banca\vir
- Cale:** C:\Users\Paul\Desktop\banca\vir
- Masca:** xx
- Scans:** 1315
- Cautare opțiuni:**
- Atribute fisiere:** Normal, Arhivat, Ascuns, Citire numai, System (checkboxes checked)
- Opțiuni:** Pattern Matching, Cautare in sub-direcție, Sortează fisiere (A-Z), Reimpresătare ListView, Use Extended Mode Scan (checkboxes checked)
- Filtrare date/dimensiune:** Dupa data: Modified, De la: 9/29/2023, la: 12/29/2023, Dim fisier: Any Size
- Scan button:** Scan
- Mai mici de limita: 1**
- File Path:** Trojan-PSW.Win32.OnLineGames.arsw | 0|AAAAAAAAAAAAA |C:\Users\Paul\Desktop\banca\vir\
- Malware Details:**

Malware Name:	Backdoor.Win32.Popwin.asc
Malware Type:	Backdoor
Content Type:	Binary
Malware Size:	20846 bytes
Danger Level:	High
- MD5:** 02bbf2879dff4e90bc64c6fbdc0c7785
- First Entry Point bytes:**
9CE8F6FFFFFF9DEBF1C2CC34FFFFF909060A40EB3C8DB55CFEFFFF8B0683F8
010FB844B020000C706010000008BD58B85F0FDFFFF2BD08995F0FDFFFF019520
- Entry Point:** LinkerVersion: 6.0, Sub System: Windows GUI, File Offset: 0000069E, Virtual Addr: 0000B000, Pointer To Raw: 0000B49E
- Functions used by this malware:** Function Role:

GetProcAddress	DLL
LoadLibrary	DLL
ExitProcess	PROCESSES
OpenProcess	PROCESSES
VirtualAlloc	RAM
VirtualFree	RAM
VirtualFreeEx	RAM
VirtualProtect	RAM
- Encrypt button:** Encrypt
- None button:** none

VIRUS ENCYCLOPEDIA



Puțin despre soluția 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

SCUT Anti Virus

Scut Ports

Process Name	State	Local IP	LPort	Remote IP	RPort	PID	Process Path
[System Idle ...	TIME_WAIT	127.0.0.1	4593	127.0.0.1	30606	0	system
[System Idle ...	TIME_WAIT	127.0.0.1	4625	127.0.0.1	30606	0	system
[System Idle ...	TIME_WAIT	127.0.0.1	4647	127.0.0.1	30606	0	system
[System Idle ...	TIME_WAIT	127.0.0.1	4649	127.0.0.1	30606	0	system
[System Idle ...	TIME_WAIT	127.0.0.1	4650	127.0.0.1	30606	0	system
chrome.exe	ESTABLISHED	127.0.0.1	4653	127.0.0.1	30606	3356	C:\Documen...
chrome.exe	ESTABLISHED	127.0.0.1	4671	127.0.0.1	30606	3356	C:\Documen...
ekrn.exe	LISTENING	127.0.0.1	30606	0.0.0.0	6323	680	C:\Program ...
[System Idle ...	TIME_WAIT	127.0.0.1	30606	127.0.0.1	4579	0	system
[System Idle ...	TIME_WAIT	127.0.0.1	30606	127.0.0.1	4580	0	system
ekrn.exe	ESTABLISHED	127.0.0.1	30606	127.0.0.1	4583	680	C:\Program ...
ekrn.exe	ESTABLISHED	127.0.0.1	30606	127.0.0.1	4671	680	C:\Program ...
[System]	LISTENING	192.168.1.2	139	0.0.0.0	2256	4	system
[System Idle ...	TIME_WAIT	192.168.1.2	4458	23.51.161.224	80	0	system
[System Idle ...	TIME_WAIT	192.168.1.2	4532	80.97.209.25	80	0	system
ekrn.exe	FIN_WAIT1	192.168.1.2	4552	173.1.98.105	80	680	C:\Program ...
[System Idle ...	TIME_WAIT	192.168.1.2	4594	80.97.208.177	80	0	system
[System Idle ...	TIME_WAIT	192.168.1.2	4627	87.240.143.2...	80	0	system
[System Idle ...	TIME_WAIT	192.168.1.2	4648	80.97.208.209	80	0	system
[System Idle ...	TIME_WAIT	192.168.1.2	4651	87.240.167.2...	80	0	system
[System Idle ...	TIME_WAIT	192.168.1.2	4652	87.240.167.2...	80	0	system
ekrn.exe	ESTABLISHED	192.168.1.2	4654	87.240.167.2...	80	680	C:\Program ...
ekrn.exe	ESTABLISHED	192.168.1.2	4672	173.194.39.1...	80	680	C:\Program ...

Anti Virus

Copyright © 2009 - 2010 Novus Ordo I.t.d. All Rights Reserved. <http://www.novusordo.ro>

SCUT Anti Virus

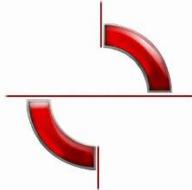
Scut CPU Monitor

Process/CPU usage/Info

PROCESS	CPU time	CPU INT	Process Info
System	0%	-	In Windows NT operating systems, the System Idle Process contains on...
smss.exe	0%	-	Session Management Subsystem - This is the process in charge of starti...
csrss.exe	0%	-	Client/server run-time subsystem - This is the user mode portion of the s...
winlogon.exe	0%	-	Microsoft Windows Logon Process - This is the process responsible for ...
services.exe	0%	-	Services Processes Controller - Services.exe is the process responsible ...
lsass.exe	0%	-	Local Security Authority Subsystem Service - is the process in charge of ...
svchost.exe	0%	-	Generic Host Process for Win32 Services - This is a generic process us...
svchost.exe	0%	-	Generic Host Process for Win32 Services - This is a generic process us...
svchost.exe	0%	-	Generic Host Process for Win32 Services - This is a generic process us...
svchost.exe	0%	-	Generic Host Process for Win32 Services - This is a generic process us...
spoolsv.exe	0%	-	Generic Host Process for Win32 Services - This is a generic process us...
explorer.exe	0%	-	Printer Spooler Service - This process job is the management of print job...
egui.exe	0%	-	Explorer.exe is the process that display Windows Explorer windows, whi...
igfxtray.exe	0%	-	[egui.exe]
hkcmd.exe	0%	-	Intel's Hotkey Command Module which gets installed by the drivers for o...
igkpers.exe	0%	-	[igfxtray.exe]
RTHDCP.EXE	0%	-	[hkcmd.exe]
igfxsrcv.exe	0%	-	[igkpers.exe]
daemon.exe	0%	-	[igfxsrcv.exe]
ctfmon.exe	0%	-	[daemon.exe]
svchost.exe	0%	-	(whose full name is Alternative User Input Services) is a Windows NT/2...
ekrn.exe	3%	CPU INT REQUEST	Generic Host Process for Win32 Services - This is a generic process us...
svchost.exe	0%	-	Generic Host Process for Win32 Services - This is a generic process us...

Anti Virus

Copyright © 2009 - 2010 Novus Ordo I.t.d. All Rights Reserved. <http://www.novusordo.ro>



Puțin despre soluția Scut Antivirus

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

Scut AntiVirus

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 Anti Virus

Scut Menu Scan Process Scut World System

Scut Process Monitor

Active processes in RAM: 57

Process Name	PID	Process Path	Memory Usage	Threads	Time	Date
alg.exe	1832	System	1012,00 KB	5	8:32	5/8/2013
av.exe	3748	C:\Program Files\Scut AntiVirus\AV\av.exe	40,09 MB	5	10:19:41	5/8/2013
chrome.exe	3356	C:\Documents and		37	5:24	5/8/2013
chrome.exe	3900	C:\Documents and		9	5:32	5/8/2013
chrome.exe	3304	C:\Documents and		20	10:17:14	5/8/2013
chrome.exe	2620	C:\Documents and		9	10:48:45	5/8/2013
cs.exe	3856	C:\Program Files\S		1	10:19:41	5/8/2013
cssrss.exe	876	System		12	8:14	5/8/2013
ctfmon.exe	448	C:\WINDOWS\system		1	5:29	5/8/2013
daemon.exe	416	C:\Program Files\U		2	5:29	5/8/2013
egui.exe	256	C:\Program Files\E		5	5:27	5/8/2013
ekrn.exe	680	C:\Program Files\E		12	5:32	5/8/2013
explorer.exe	184	C:\WINDOWS\Exp		22	5:25	5/8/2013
filezilla.exe	2676	C:\Program Files\F		3	7:46:26	5/8/2013
fw.exe	3776	C:\Program Files\S		4	10:19:41	5/8/2013
hkcmd.exe	276	C:\WINDOWS\system		2	5:28	5/8/2013
igfxpers.exe	300	C:\WINDOWS\system32\igfxpers.exe	252,00 KB	3	5:28	5/8/2013
igfxsrvc.exe	384	C:\WINDOWS\system32\igfxsrvc.exe	1,61 MB	2	5:28	5/8/2013
igfxtray.exe	272	C:\WINDOWS\system32\igfxtray.exe	312,00 KB	4	5:28	5/8/2013
in.exe	3688	C:\Program Files\Scut AntiVirus\IN.exe	19,67 MB	4	10:52:2	5/8/2013
ip.exe	2128	C:\Program Files\Scut AntiVirus\IP.exe	18,82 MB	1	10:52:3	5/8/2013
ksvc.exe	n/a	C:\WINDOWS\system32\ksvc.exe	4,07 MB	20	5:28:10	5/8/2013

RTHDCPL.EXE is not infected !
The file C:\WINDOWS\RTHDCPL.EXE is NOT infected !

Scut Proactive AntiVirus

Real Time Help

Every computer us SCUT antivirus is generally called SC is part of it.

Anti Virus Fire Wall Status Report Tools Options Support Update

<http://www.novusordo.ro>

SCUT Anti Virus

Scut Menu Proactiv Firewall Scut World System

Proactiv Firewall

Connection Locator Connection Detail Connection Sniffer Connection Tracer Port Scan

Real Time Help

Click here for definitions update, viral definitions, heuristic definitions, TDS definitions and IDS definitions. Also choose the connection type, update type and the parameters for update.

Firewall

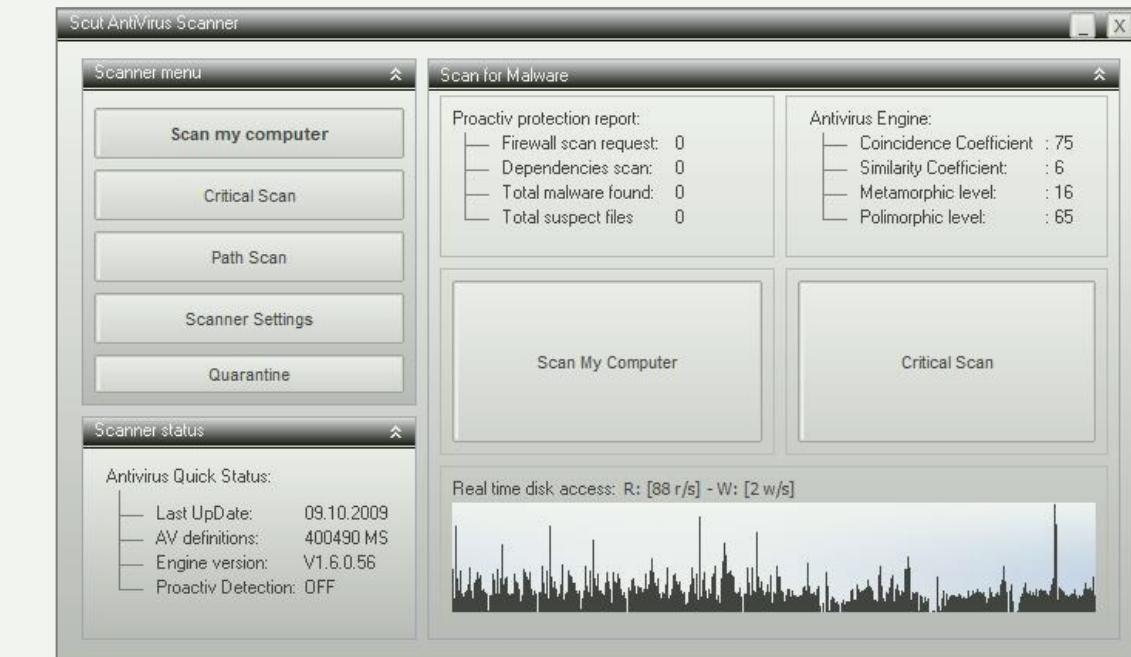
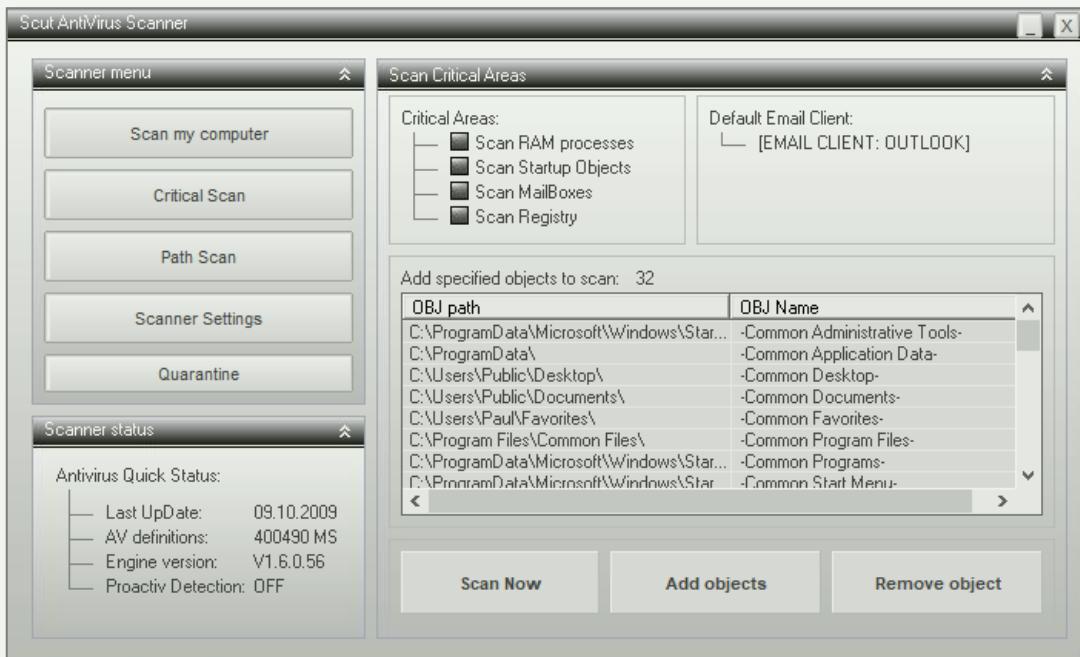
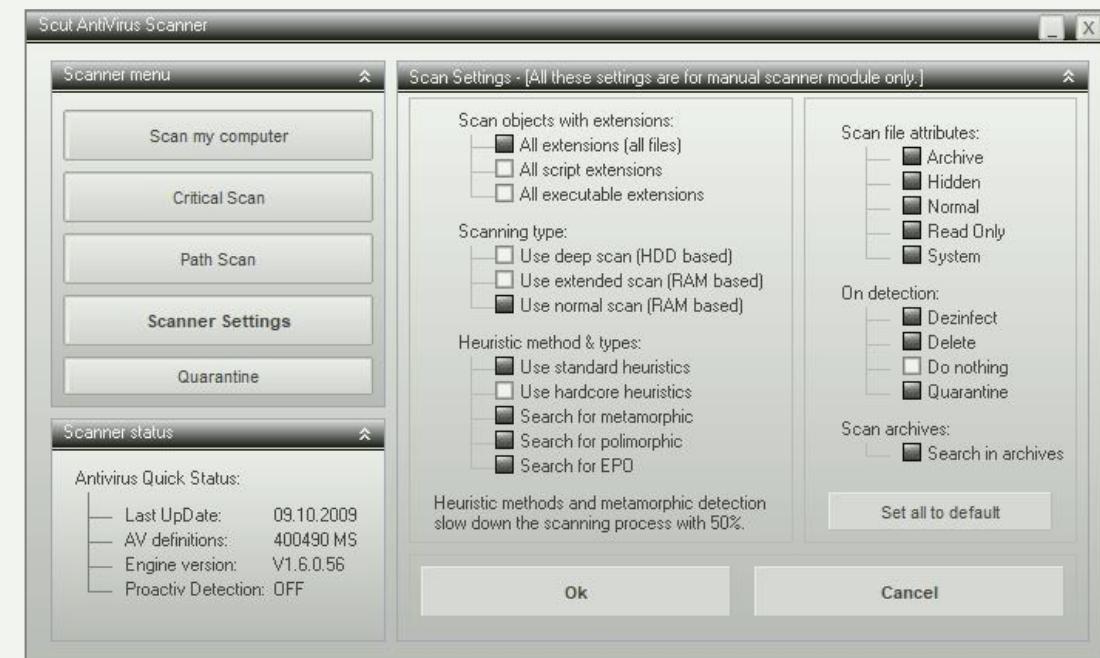
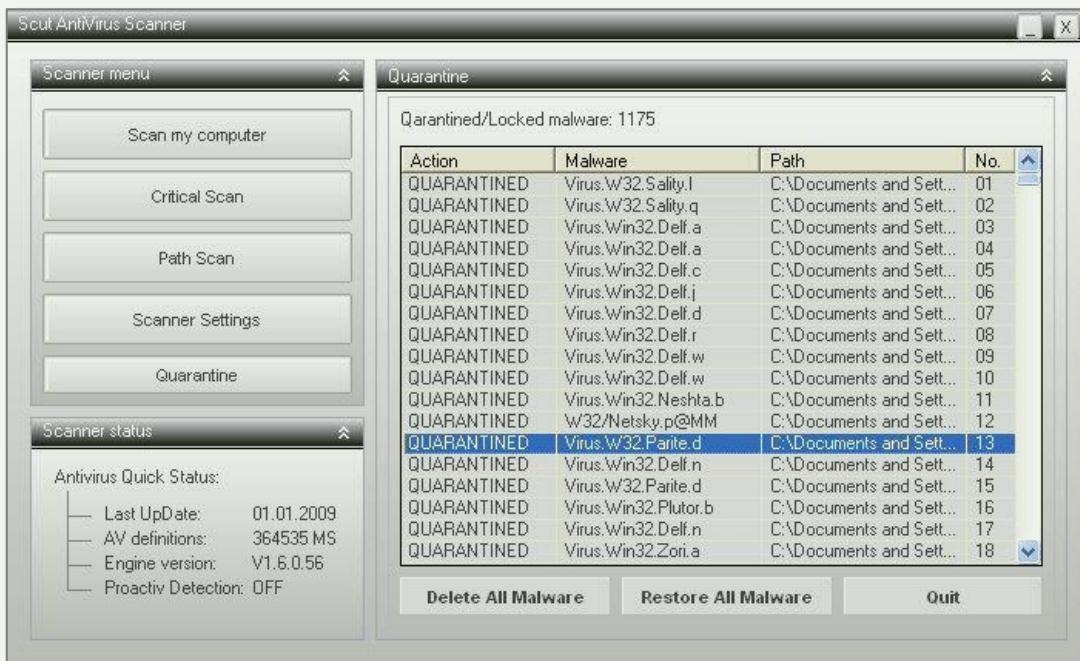
Tactical Defence Response

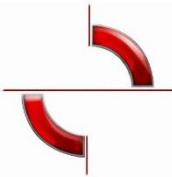
Scann senzor

Tactical Defence Response

Anti Virus Fire Wall Status Report Tools Options Support Update

Copyright © 2009 - 2010 Novus Ordo I.t.d. All Rights Reserved. <http://www.novusordo.ro>





Puțin despre soluția Scut Antivirus

Scut AntiVirus

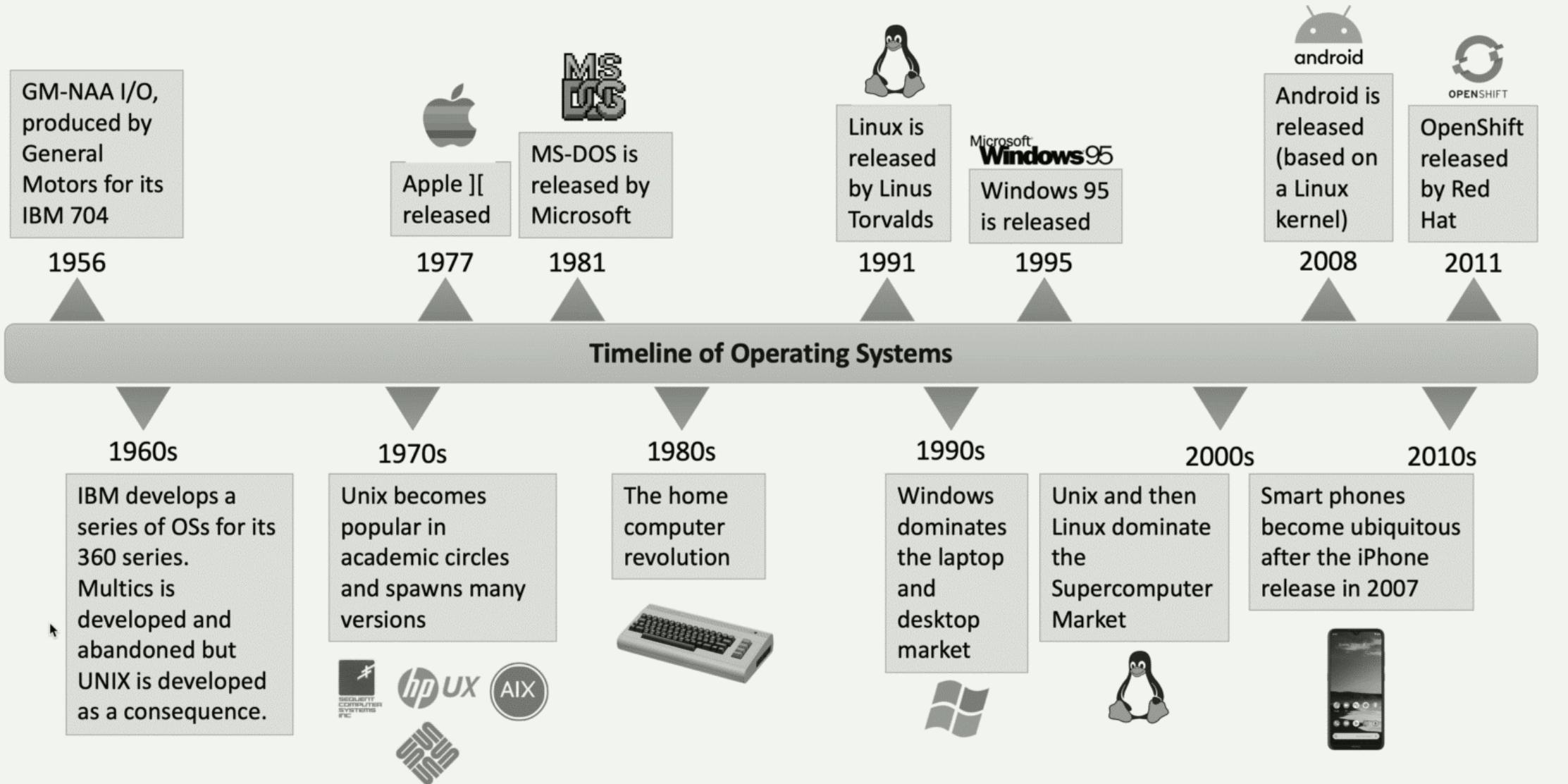


C.1.4

SISTEMELE DE OPERARE ȘI STRATUL DE PORTABILITATE

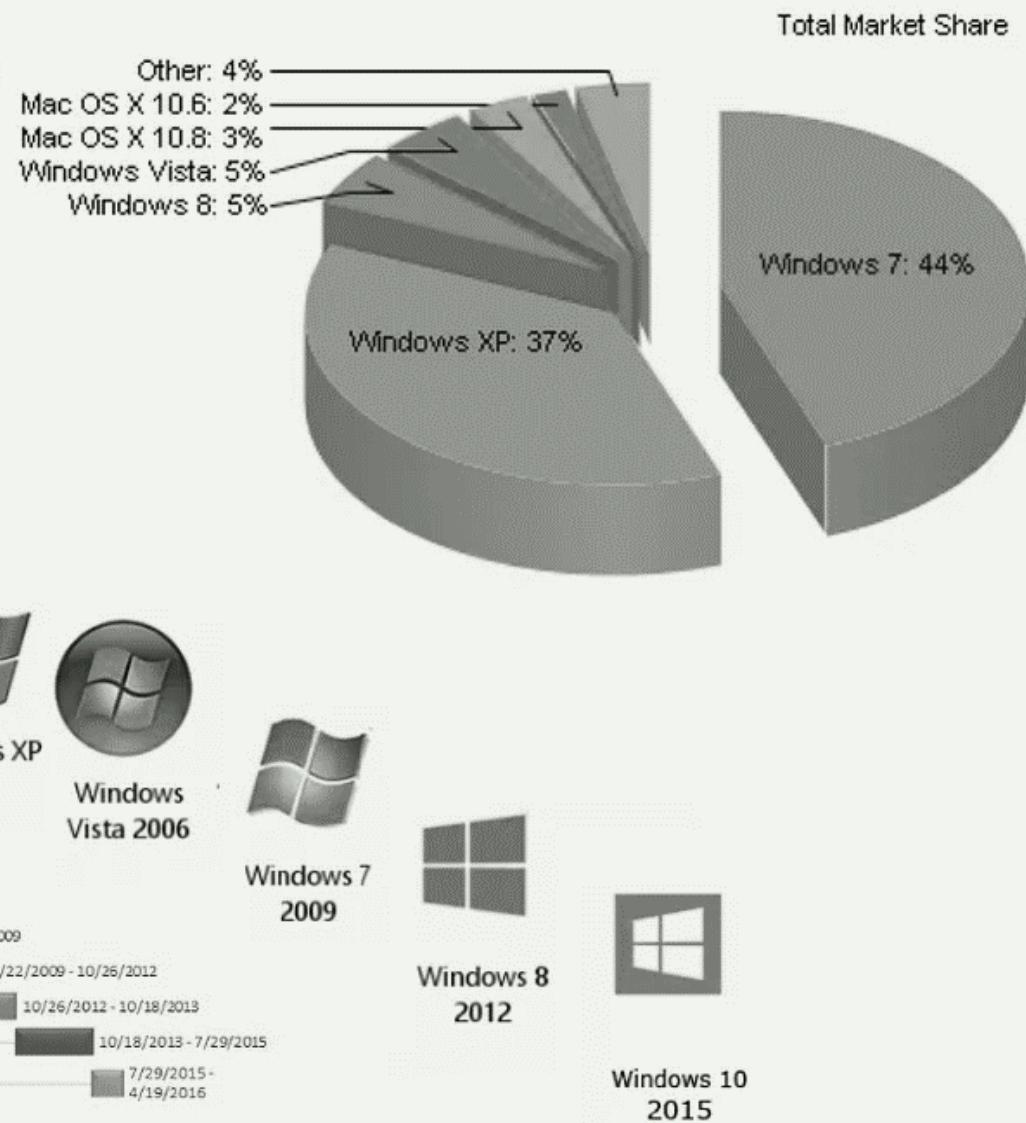
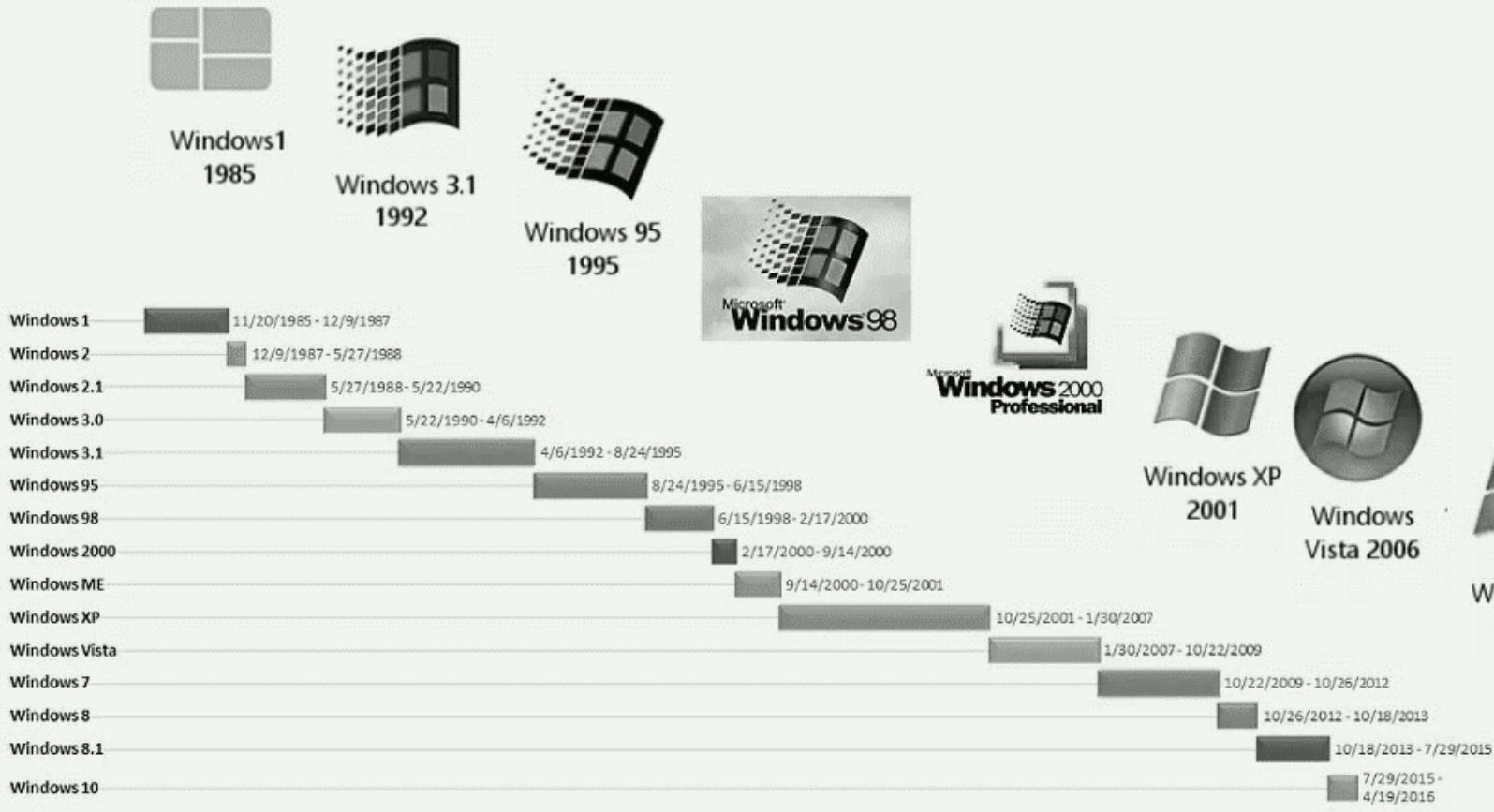


Sistemele de operare în timp



Windows Operating Systems

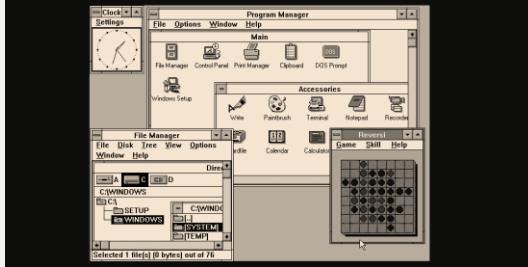
VERSION RELEASE DATE AND LIFECYCLE



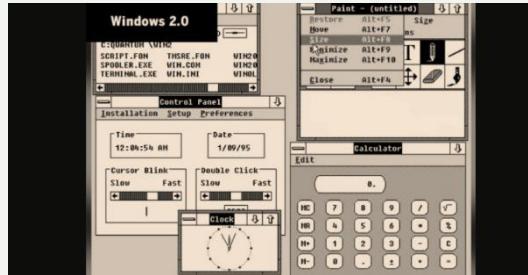
1985 1989 1993 1997 2001 2005 2009 2013 2016

Structura OS a dictat varianta de malware

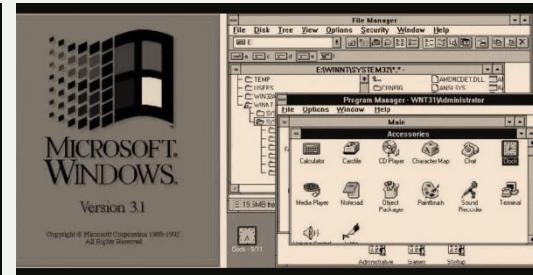
Windows 1



Windows 2.0



Windows 3.1



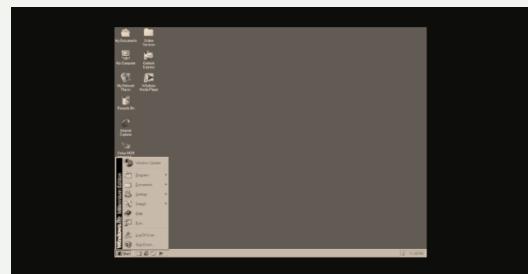
Windows 95



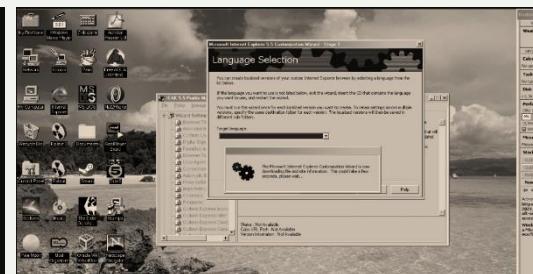
Windows 98



Windows 2000



Windows NT



Windows XP



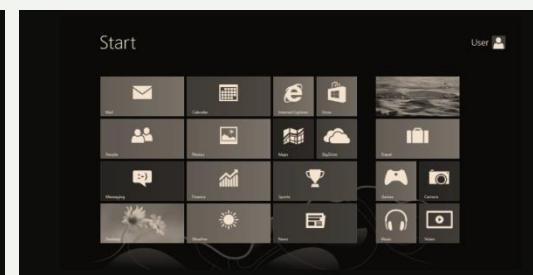
Windows 7



Windows Vista



Windows 8.0



Windows 10

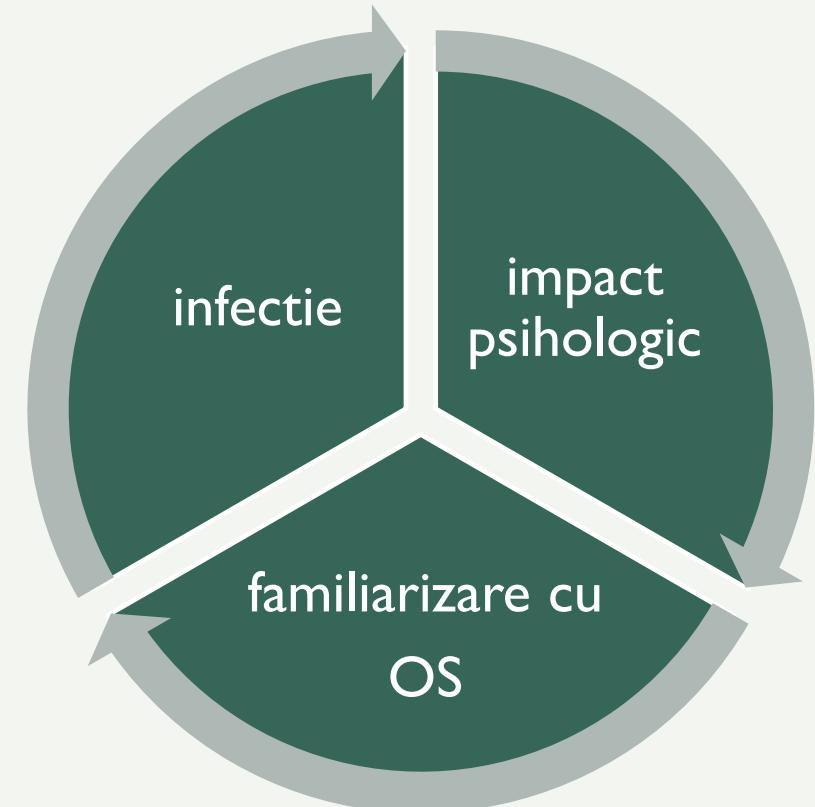


PERSISTENȚA SISTEMULUI DE OPERARE WINDOWS

RESPECTAREA LEGILOR NATURII

In masinile biologice, virus+host=evolutie

- Sistemele de operare care nu pot fi infectate, dispar!
- Infectia este o metodă evolutivă de îmbunătățire a sistemului de operare.
- Infectia 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!



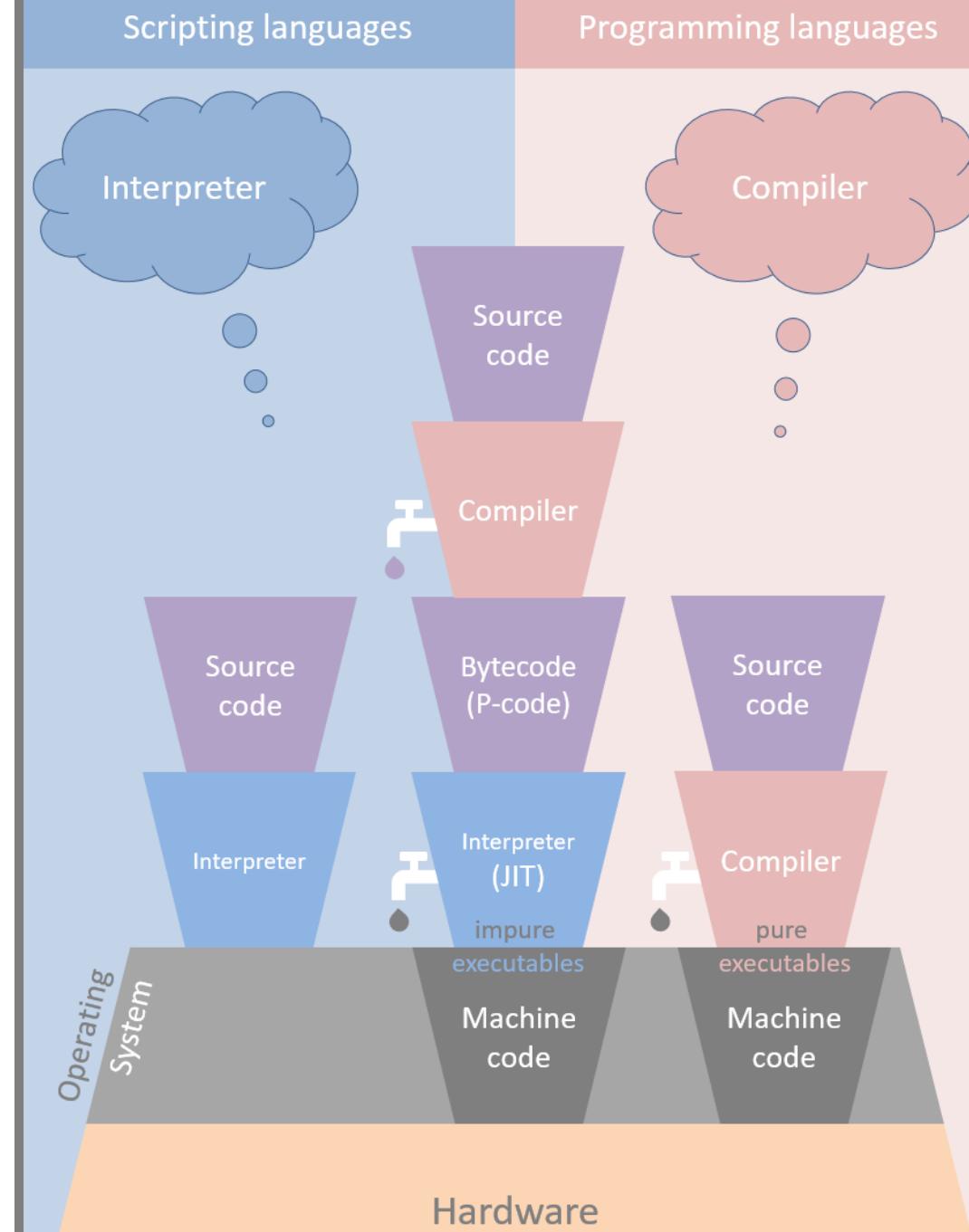
De ce ransomware este viitorul malware?

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

Se face distincția intre:

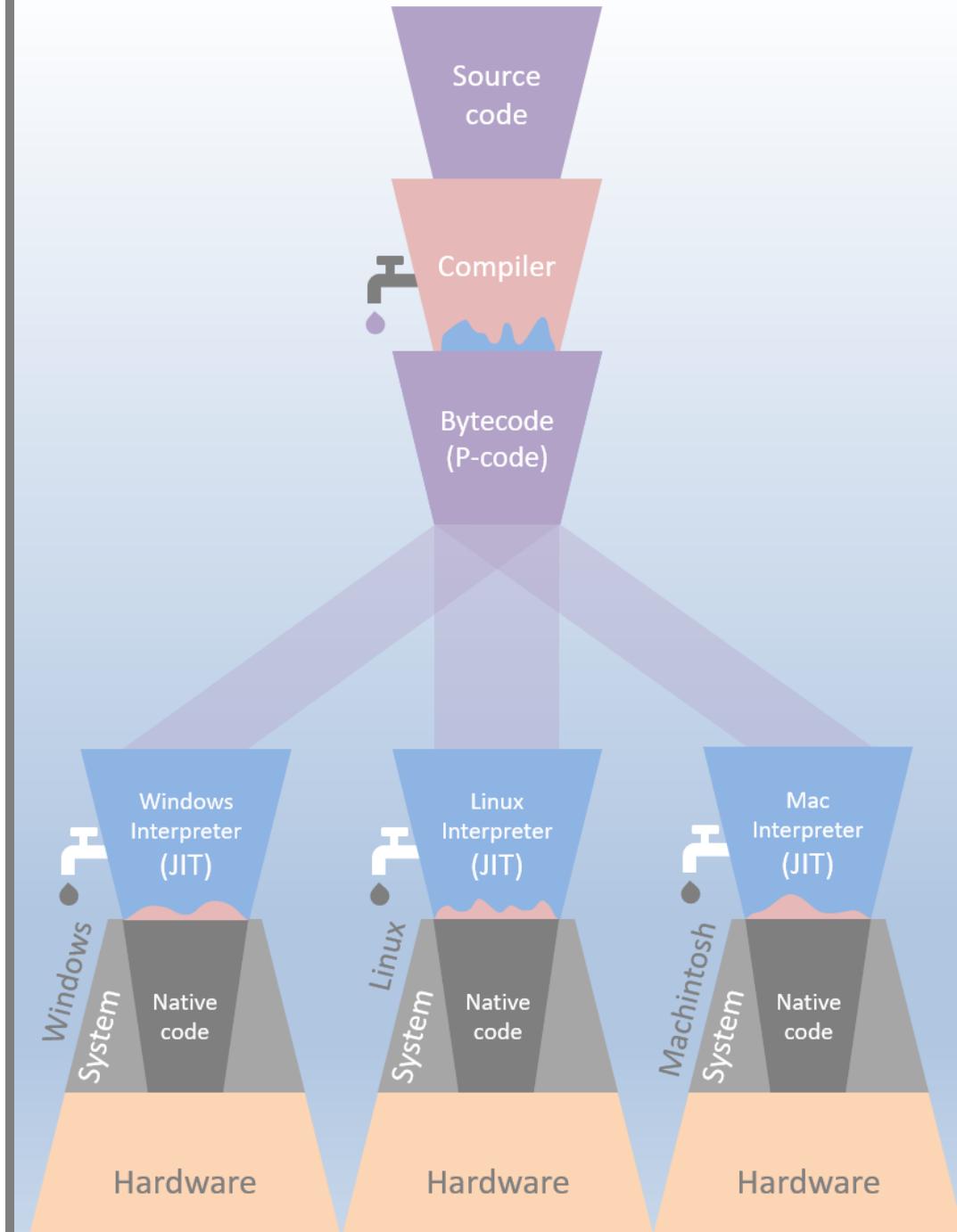
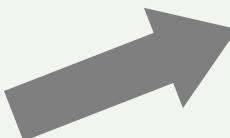
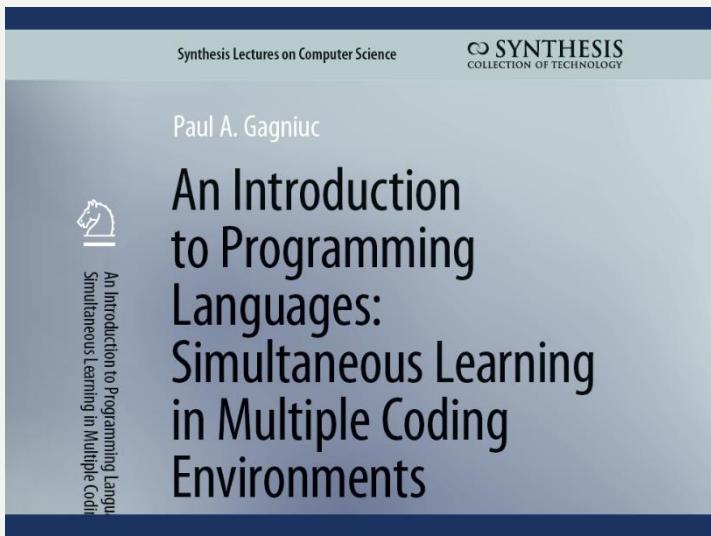
- Executabil – self (nativ)
- Executabil - non-self (hibrid)

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



Directia organizării software

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



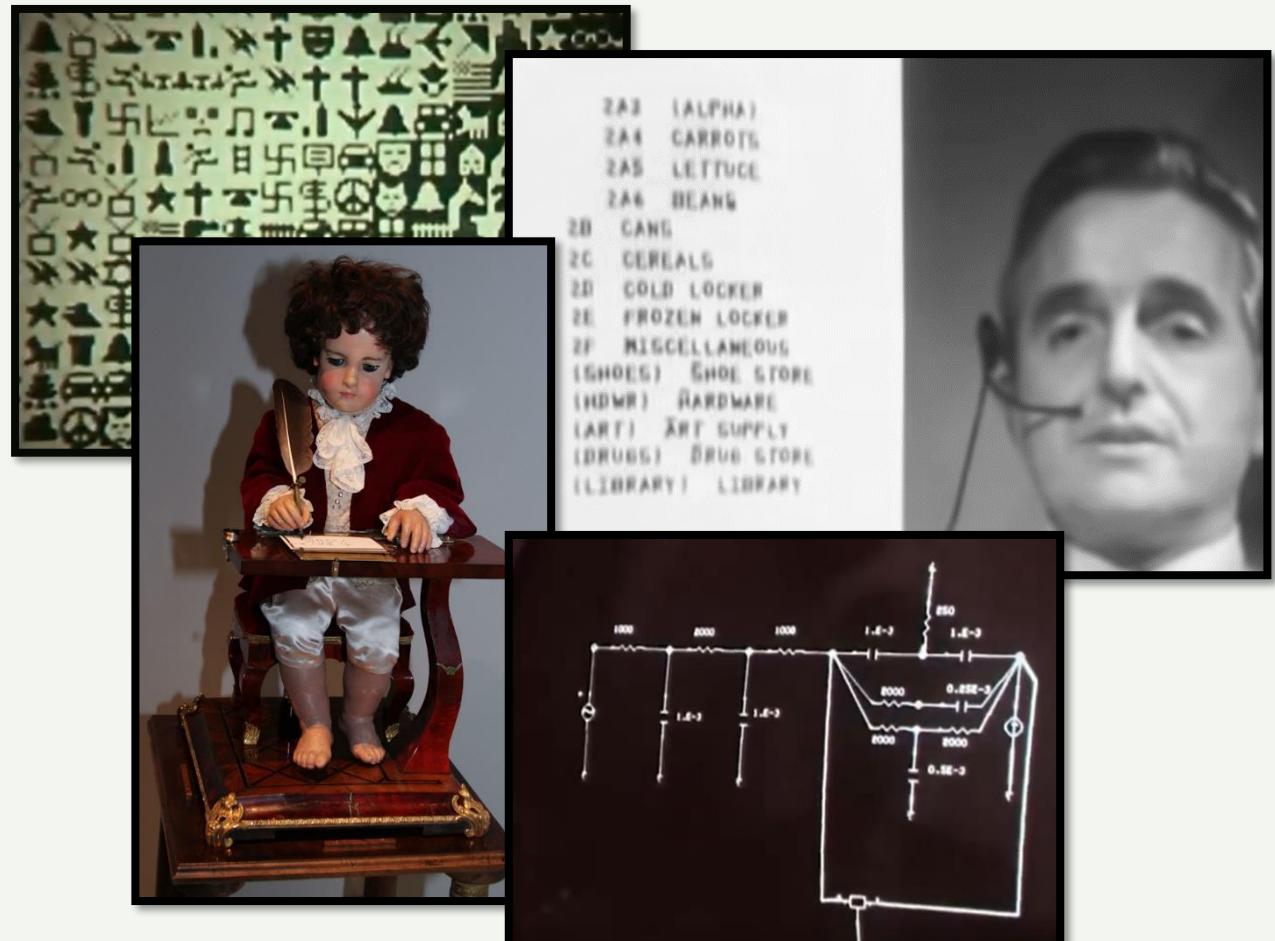
CONCLUZII

- 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>

