

# C.3 CLASE MALWARE: STRUCTURĂ ȘI FUNCȚIONALITATE

PAUL A. GAGNIUC



Academia Tehnică Militară „Ferdinand I”

# **PRINCIPALELE PĂRȚI ALE PREZENTĂRII (1)**

---

## **C.3 Clase Malware: structură și funcționalitate:**

- **C.3.1 LIMBAJE COMPUTERIZATE ȘI MOTIVAȚIA PROIECTĂRII MALWARE**
- **C.3.2 SISTEMUL DE OPERARE DIN PERSPECTIVA APLICAȚIILOR MALWARE**
- **C.3.3 CLASE DE MALWARE**
- **C.3.4 NOTAȚIA FOLOSITĂ PENTRU DENUMIREA APLICAȚIILOR MALWARE**
- **C.3.5 VALABILITATEA BĂNCII MALWARE ȘI POLIMORFISM VS METAMORFISM**

# **PRINCIPALELE PĂRȚI ALE PREZENTĂRII (2)**

---

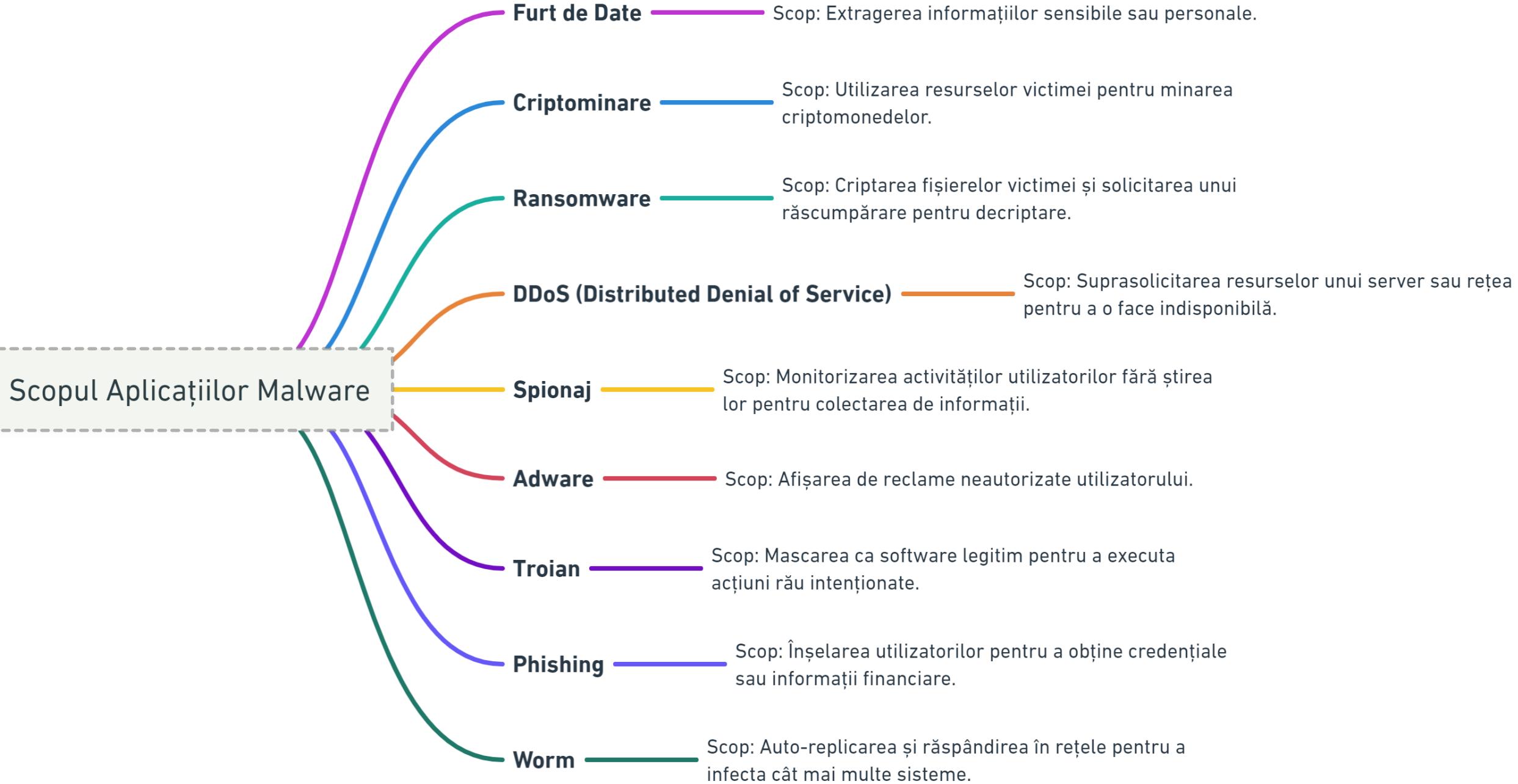
## **C.3 Clase Malware: structură și funcționalitate:**

- **C.3.6 CRIPTOGRAFIE, PERSISTENȚĂ, OFUSCARI ȘI EXPLOATĂRI**
- **C.3.7 APLICAȚII DE INFILTRARE: BACKDOOR ȘI DROPPER**
- **C.3.8 TIPURI DE TROIENI ȘI METODELE LOR DE INFECTARE**
- **C.3.9 TIPURI DE VIERMI ȘI METODELE LOR DE INFECTARE**
- **C.3.10 TIPURI DE VIRUȘI, CICLUL LOR DE VIAȚĂ ȘI METODE DE INFECTARE**

C.3.1

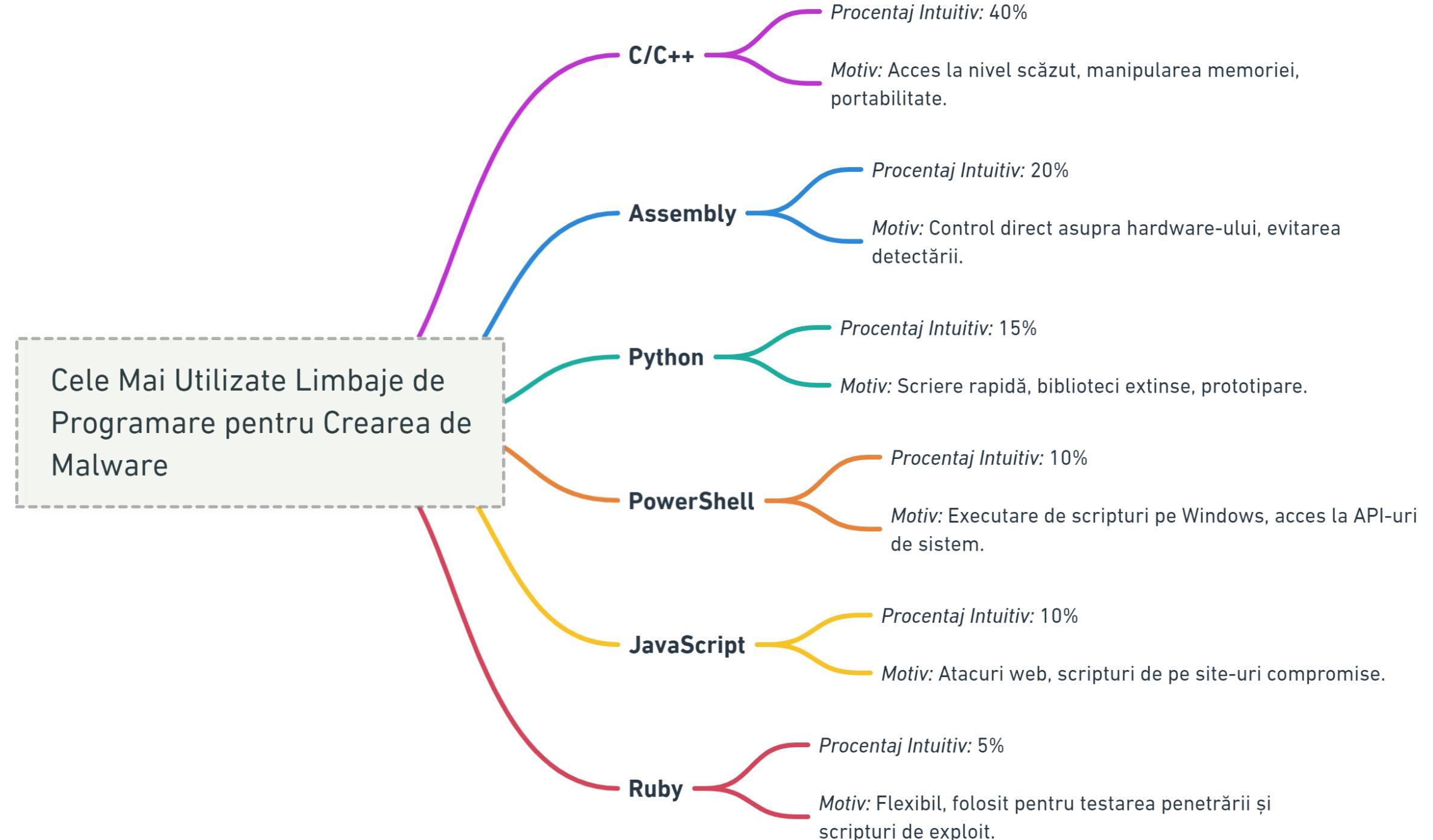
# LIMBAJE COMPUTERIZATE ȘI MOTIVATIA PROIECTĂRII MALWARE







## Cele Mai Utilizate Limbaje de Programare pentru Crearea de Malware



C.3.2

# SISTEMUL DE OPERARE DIN PERSPECTIVA APLICAȚIILOR MALWARE







ntdll.dll contribuie direct la configurarea „coconului” intern al noului proces .exe. Mai precis, ea participă la setarea tuturor structurilor critice care definesc contextul intern de execuție al acelui proces în modul utilizator.

## Biblioteci Windows Frecvent Exploatate de Malware

- ntdll.dll este responsabilă pentru inițializarea bazală a procesului, creând contextul intern necesar — heap-ul, TEB (Thread Environment Block), PEB (Process Environment Block), tabela de excepții (SEH), și traducerea apelurilor în syscall către kernel.
- Practic, biblioteca ntdll.dll construiește „mediul de rulare” minimal în care codul aplicației poate funcționa, înainte ca kernel32.dll sau runtime-ul C să preia controlul.

**user32.dll** — Descriere Exploatare: Injectarea de cod prin "DLL Injection"

**kernel32.dll** — Descriere Exploatare: Manipularea proceselor și a memoriei

**ntdll.dll** — Descriere Exploatare: Interacțiune directă cu Kernelul Windows

**shell32.dll** — Descriere Exploatare: Execuția de comenzi sau lansarea aplicațiilor

**ws2\_32.dll** — Descriere Exploatare: Comunicații de rețea, exfiltrarea datelor

**advapi32.dll** — Descriere Exploatare: Modificarea registrelor și obținerea de privilegii

**crypt32.dll** — Descriere Exploatare: Criptografie, criptarea fișierelor sau comunicarea securizată

**oleaut32.dll, ole32.dll** — Descriere Exploatare: Execuția de cod arbitrar prin obiecte OLE

**gdi32.dll, win32k.sys** — Descriere Exploatare: Atacuri pentru escaladarea de privilegii sau evitarea izolării proceselor



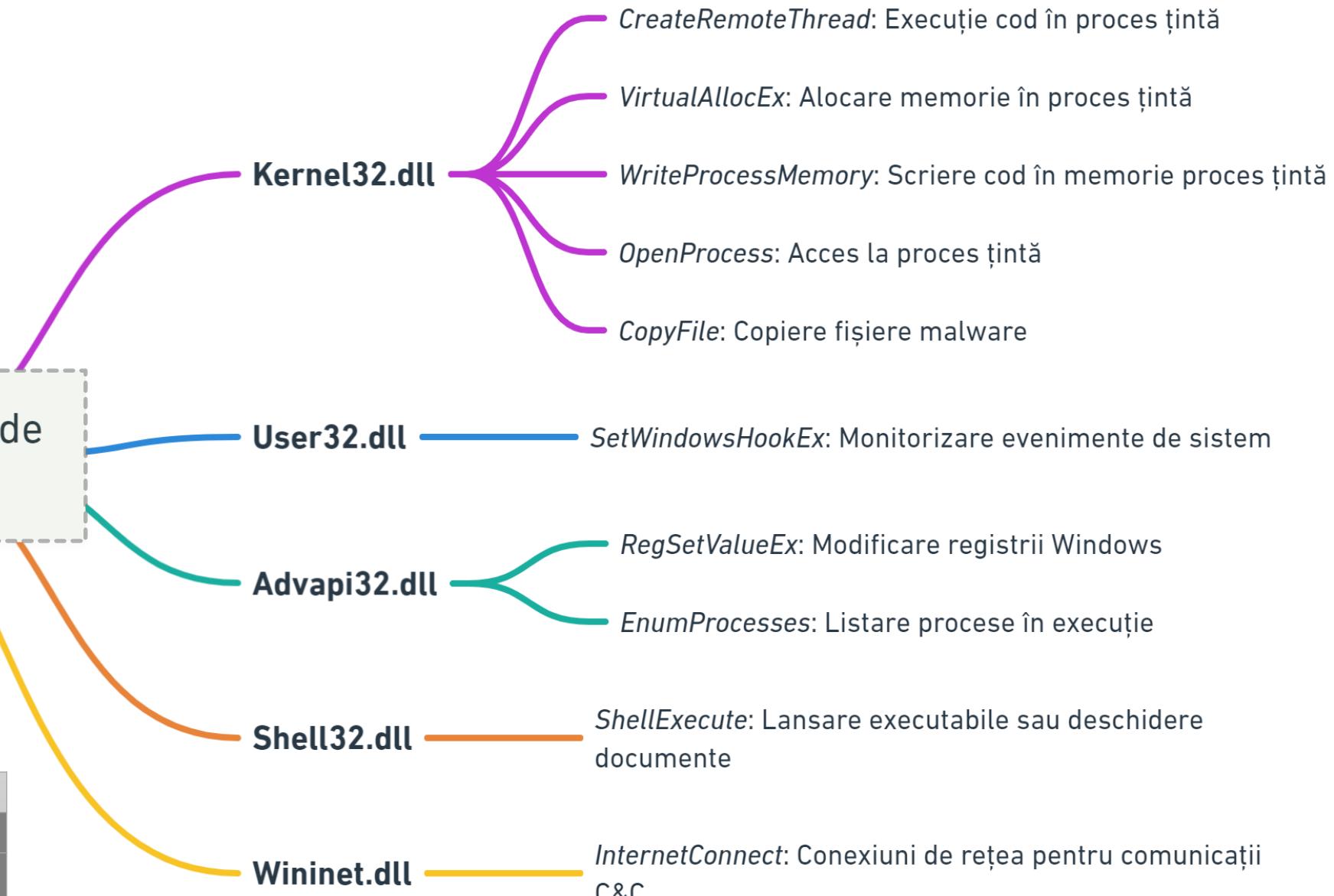
În API-urile Windows, sufixul **Ex** vine de la “**Extended**”, adică o versiune extinsă a unei funcții deja existente.

## DLL-uri și Funcții API Folosite de Malware

Funcțiile cu **Ex** au fost introduse pentru a oferi control mai detaliat sau funcționalitate suplimentară, fără a rupe compatibilitatea cu versiunile vechi de Windows sau aplicații existente.

### De exemplu:

CreateWindow	Creează o fereastră cu opțiuni de bază.
CreateWindowEx	Adaugă parametru în plus pentru extended window styles (dwExStyle) → permite transparență, ferestre tool-tip, ferestre care nu apar în taskbar etc.





Application Programming Interface

### Funcții API Cele Mai Folosite de Malware în DLL-uri

#### Exemplu de subset

(pattern clasic de injecție remote):

- OpenProcess → accesează un alt proces (victimă),
- VirtualAllocEx → alocă memorie în acel proces,
- WriteProcessMemory → injectează shellcode sau DLL path,
- CreateRemoteThread → pornește execuția codului injectat.

Acest lanț este o **semnatura comună** pentru troieni, RAT-uri (Remote Access Trojans), loadere, și infectii de tip **fileless**.

**CreateRemoteThread** — Descriere: Permite malware-ului să execute cod în cadrul unui proces țintă.

**VirtualAllocEx** — Descriere: Alocă memorie într-un proces țintă pentru injectarea de cod.

**WriteProcessMemory** — Descriere: Scrie codul malware în memoria alocată a unui proces țintă.

**SetWindowsHookEx** — Descriere: Instalează un hook pentru a monitoriza evenimentele de sistem și a executa codul malware ca răspuns.

**RegSetValueEx** — Descriere: Modifică valorile din registrii Windows pentru persistență sau modificarea setărilor de securitate.

**OpenProcess** — Descriere: Obține acces la un proces țintă pentru manipulare.

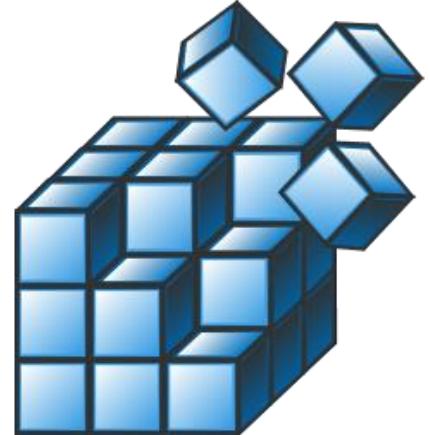
**EnumProcesses** — Descriere: Listează procesele în execuție pe sistem pentru a identifica ținte potențiale.

**CopyFile** — Descriere: Copiază fișiere malware în locații specifice pentru distribuție sau infectare.

**ShellExecute** — Descriere: Lansează executabile sau deschide documente, util în fazele inițiale de infectare sau pentru a executa alte programe malware.

**InternetConnect** — Descriere: Stabilă conexiuni de rețea pentru comunicări cu serverele de comandă și control sau pentru exfiltrarea datelor.

- Un handle este un identificator folosit de sistemele de operare pentru a referi resurse sistem, cum ar fi fișiere, ferestre, conexiuni la internet sau procese.
- Este practic un număr sau un token unic care "mânuiește" referința către un obiect sau o resursă în memoria sistemului, permitând software-ului să acceseze și să manipuleze acea resursă printr-o interfață standardizată.
- Prin folosirea handle-urilor, aplicațiile nu trebuie să interacționeze direct cu adresele de memorie sau cu structurile de date interne ale sistemului de operare, ceea ce simplifică dezvoltarea software-ului și protejează integritatea sistemului și a datelor.



### Zone de Interes pentru Malware în Registrii Windows

#### Handle



## Etimologie (De unde vine "d" din httpd.exe?):

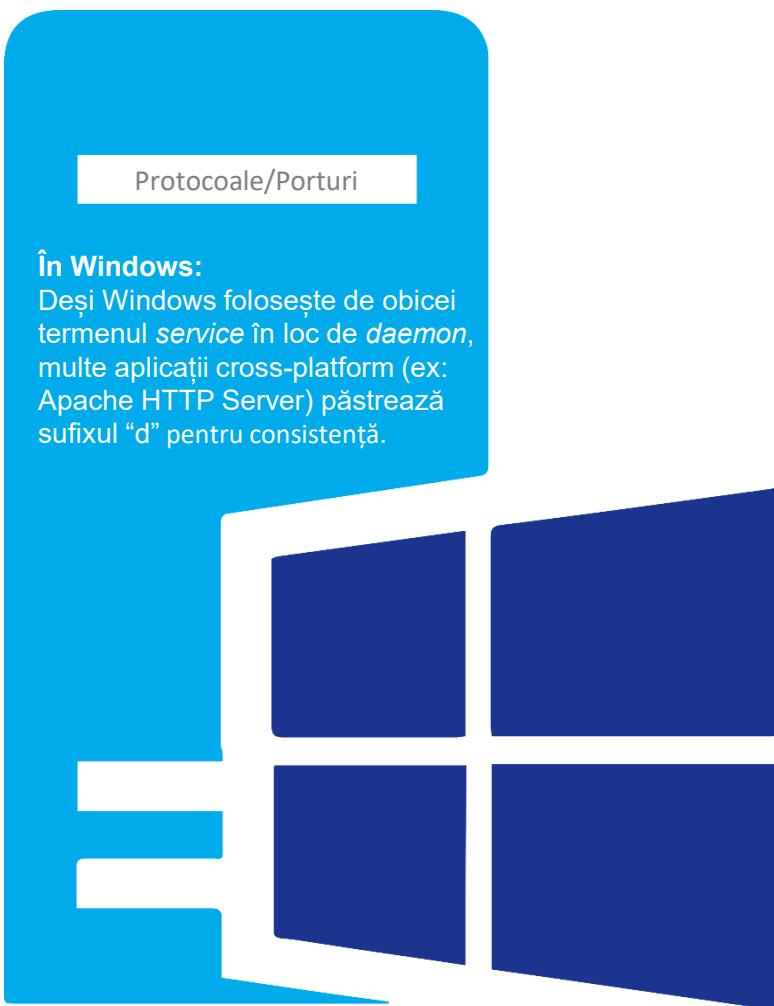
- **http** – protocolul de comunicare (HyperText Transfer Protocol).
- **d** – prescurtare de la **daemon** (sau „demon”, în sensul Unix-like), adică un proces server care ascultă cereri pe portul HTTP (de obicei portul 80 sau 443).

## Exemple similare:

**sshd** – Secure Shell Daemon – serverul SSH.

**ftpd** – File Transfer Protocol Daemon – server FTP.

**mysqld** – MySQL Daemon – serverul de baze de date MySQL.



**C.3.3**

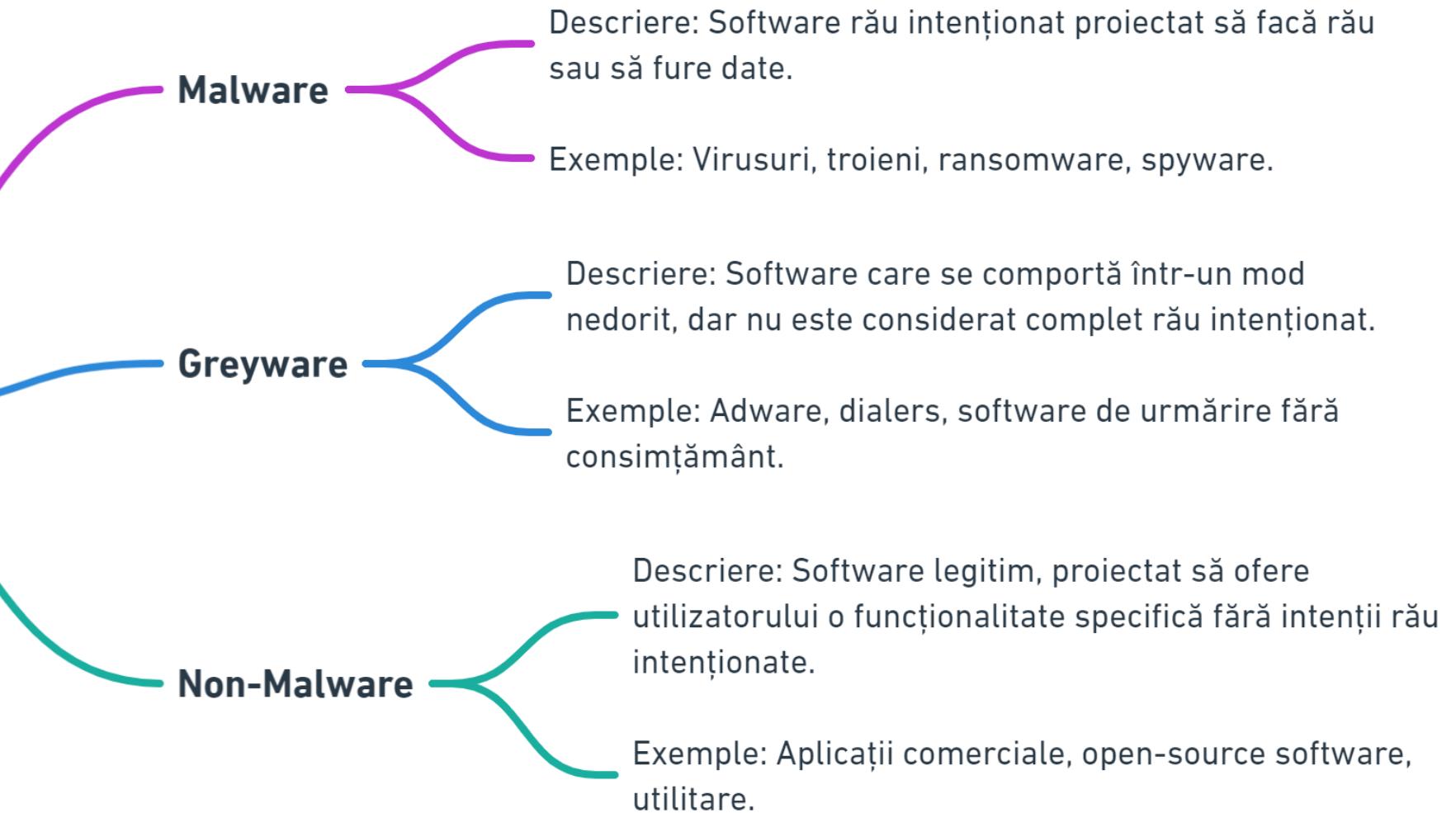
# **CLASE DE MALWARE**



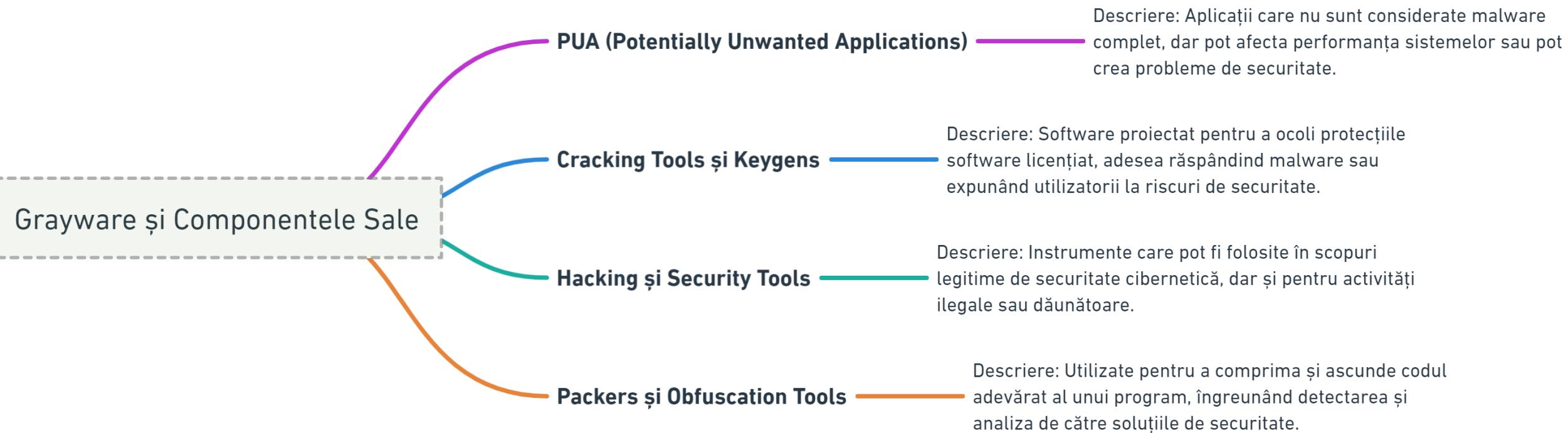


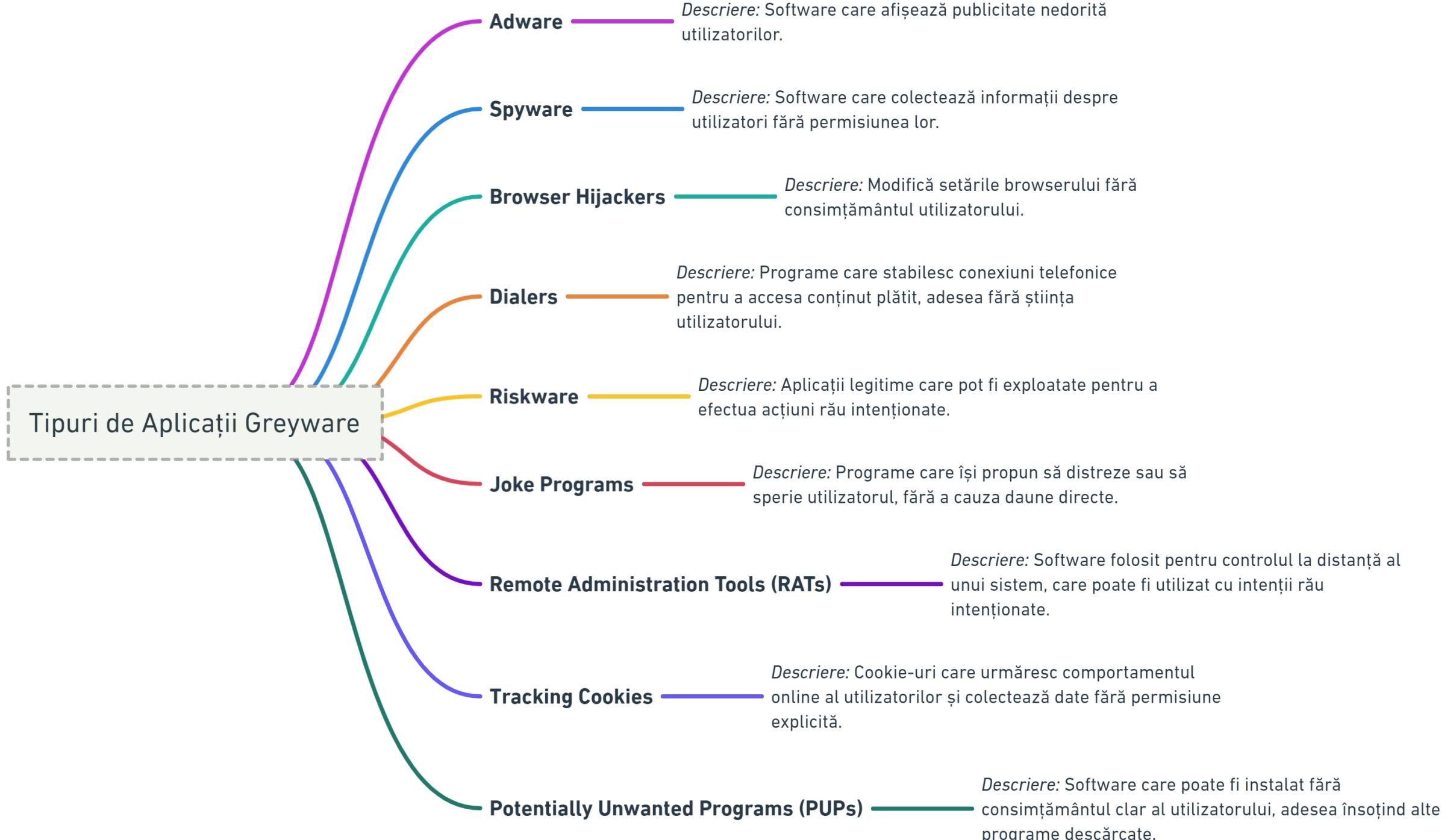
- Malware**
  - Viruși*: Infectează fișiere pentru a se auto-replica.
  - Troieni*: Maschează intenții rău intenționate sub aparența unei aplicații legitime.
  - Ransomware*: Criptează datele utilizatorului și solicită răscumpărare.
  - Spyware*: Colecțează informații despre utilizator fără consimțământ.
  - Adware*: Afisează reclame nedorite.
  - Worms*: Se auto-replică fără a infecta alte fișiere.
  - Rootkits*: Ascunde alte activități malware.
  - Bots*: Parte a unei rețele de botneturi pentru atacuri DDoS sau spam.
- Non-Malware**
  - Aplicații de Productivitate*: Procesare text, foi de calcul.
  - Instrumente de Dezvoltare*: IDE-uri, compilatoare.
  - Software de Securitate*: Antivirus, firewall-uri.
  - Jocuri*: Pentru divertisment.
  - Aplicații de Comunicații*: E-mail, mesagerie instant.
  - Aplicații Multimedia*: Playere video și audio, editare foto și video.
  - Utilitare de Sistem*: De optimizare, curățare și întreținere.

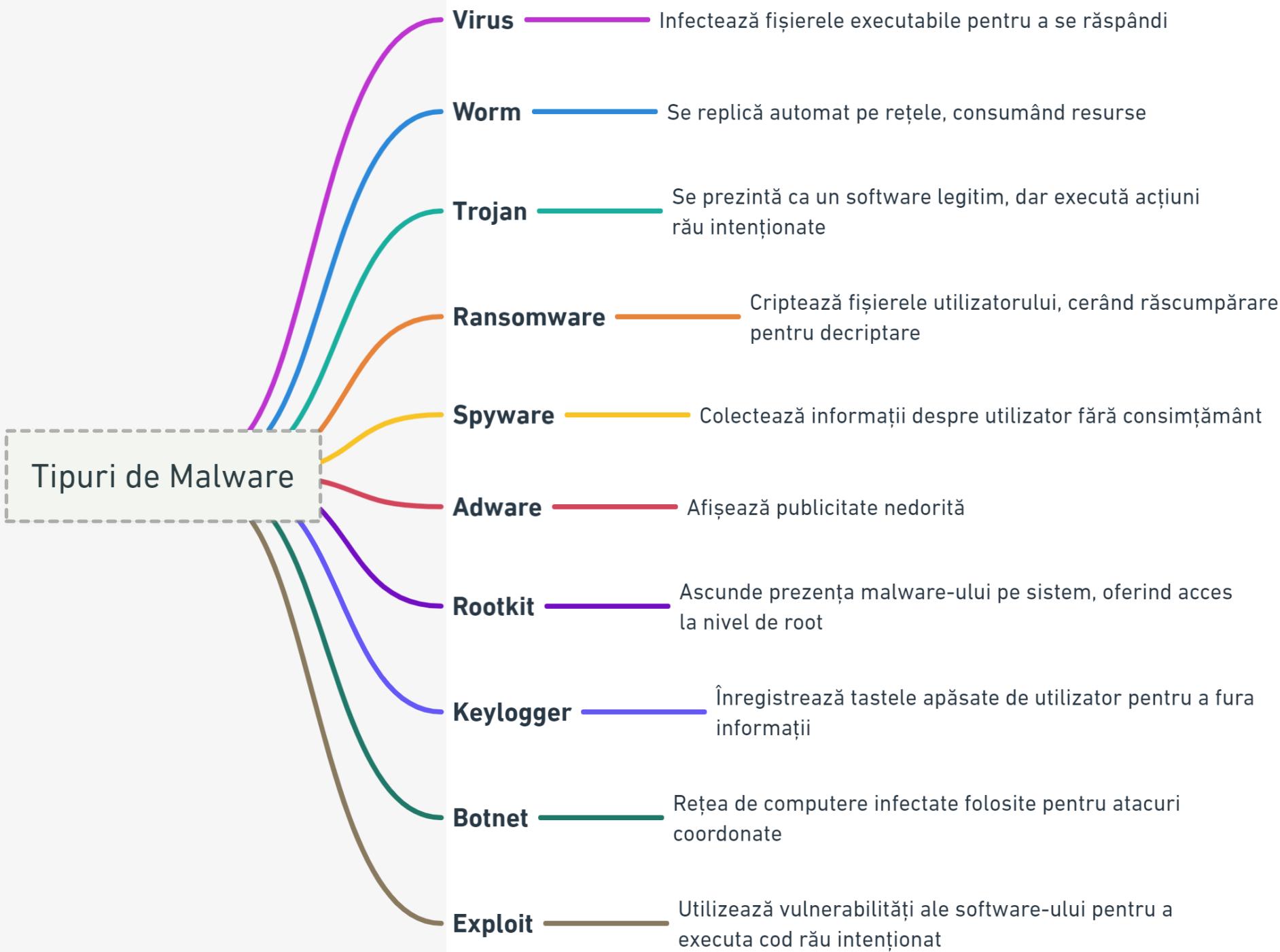
## Clasificarea Aplicațiilor



Motivația pentru detecție: Protejarea computerelor în companii sau instituții militare!







C.3.4

# NOTAȚIA FOLOSITĂ PENTRU DENUMIREA APLICAȚIILOR MALWARE



# Notația folosită (1)

Class.SubClass.Name.Variant

Backdoor.Win32.Tiny.A

Unde „Backdoor” este clasa principală, „Win32” reprezintă una dintre cele patru subclase, și anume „[OS]”. De asemenea, „Tiny” este MUS, care este sirul găsit în fișierul malware (de obicei semnătura scriitorului de malware inserată intenționat pentru mândrie), iar MVN este „A”, care în acest caz reprezintă prima variantă. Întrebarea aici este: Dar de ce „A” pentru variantă? Ei bine, alte programe malware pot avea sirul „Tiny” în conținutul fișierelor lor, astfel, eticheta de variantă va permite o diferențiere.



[MKN] Malware Known Name (if the malware has a stable file name),  
[MEN] Malware Effects Name (the effects they cause after execution),  
[MUS] Malware Unique String (unique string found inside the malicious file),

[PCN] Polymorphic Core Name (one version with multiple forms of itself),  
[MCN] Metamorphic Core Name (one version with multiple file types),  
[MVN] Malware Variant Name (packagings and compilations of the same malware)

Class (generic)	SubClass				Name	Variant
	[FT]	[AT]	[SP]	[OS]		
Virus	JS	Boot	IM	DOS	MKN	MCN
Trojan	SWF	Clicker	IRC	Win16	MEN	PCN
Exploit	ASP	Nuker	Net	Win32	MUS	MVN
Backdoor	VBS	Dialer	P2P	Win64		
Keylog	BAT/CMD	DoS	Email	Linux		
Worm	PHP	DDoS	SMS	UNIX		
HackTool	VBA	Downloader	Unclassified	SymbOS		
RootKit	HTM	Dropper		Mac		
Adware	MTH	Flooder		WinCE		
Spyware	XML	GameThief				
Malware	CSS	Notifier				
	INF	Proxy				
	EXE	Sniffer				
	REG	Spam				
	Perl	Spoof				
	MSExcel	Spy				
	MSOffice	RCE				
	MSWord	VirTool				
	Unclassified	Constructor				
		Unclassified				

Class[1...11].SubClass[Type{1...4}].Name[Type{1...3}].Variant[Type{1...3}]

[FT] File Type SubClass, [AT] Action Type SubClass, [SP] Spreading Pathway SubClass, [OS] OS name SubClass.

# Notația folosită (2)

---

În urma acestui raționament, o a doua versiune va fi marcată cu „B” și aşa mai departe. Pentru a da un alt exemplu, rețineți că în:

Trojan.Win32.Kebede.I

Varianta „I” înseamnă că a fost detectată versiunea 9 a troianului numit „Kebede”, deoarece „I” este a noua literă din alfabet, în timp ce:

Trojan.Win32.Kebede.AB

Înseamnă că detecția reprezintă troianul Kebede, versiunea 28. Asta pentru că se pot nota 26 de variante folosind cele 26 de litere ale alfabetului, iar când apare varianta 27 se folosește varianta de notație „AA”, ceea ce înseamnă  $26+1=27$ . Când apare versiunea 28, notația devine „AB”, ceea ce înseamnă  $26+2=28$ . Aceasta este similară cu notația coloanei din Excel.

Evident, notația se poate baza pur și simplu pe reprezentarea întregului în care:

*Trojan.Win32.Kebede.AB ... devine ... Trojan.Win32.Kebede.28*

Cu toate acestea, notația folosind numere este departe de a fi elegantă. Astfel, totul se bazează pe sistemul de referință al laboratorului (vă rog să rețineți că notația de mai sus este făcută pentru oameni și este adevărată pentru *Scut Antivirus*). În același sens, „AA” poate însemna  $1+1=2$  care poate fi, de asemenea, echivalent cu „B” care este direct 2, sau „AA” poate însemna 11; de asemenea „WW” poate însemna  $26+26=52$  sau „WW” poate însemna și 2626.).

# Notația folosită (3)

---

Pentru a oferi un ultim exemplu cu notația variantă aşa cum este descrisă pentru Scut Antivirus, un virus de computer poate fi notat ca:

Virus.Win32.Virut.BH

Unde „BH” este varianta 60 a virusului informatic numit Virut, care infectează sistemele de operare Win32 (rețineți că varianta BH a lui Virut nu există, este doar un exemplu). Dar dacă virusul este polimorf și nu are șiruri distinctive în conținutul său? Ei bine, aşa cum este specificat mai sus pentru MCN și PCN, fie cercetătorul de securitate oferă un nume potrivit pentru acel program malware specific, fie poate adăuga un nume implicit, cum ar fi „p@” pentru polimorf necunoscut, sau „m@” pentru un metamorfic necunoscut:

Virus.Win32.p@.D

Ceea ce înseamnă că este a patra variantă descoperită a unui virus polimorf care infectează sistemele Win32. Acest lucru poate fi prea scurt și confuz, deoarece există mulți viruși polimorfi, prin urmare, ar trebui furnizat un nume distinctiv pentru a evita confuziile viitoare. Astfel, cercetătorul de securitate poate furniza un nume și semnătura polimorfă necunoscută, cum ar fi:

Virus.Win32.NetSky.p@.D

# Notația folosită (4)

---

Rețineți că, chiar dacă numele este, din greșeală, același pentru mai multe tipuri de malware, acest lucru nu afectează detectarea, deoarece numele sunt importante pentru profesionistul în securitate și sunt irelevante pentru metodele de detectare utilizate. Astfel, cerul este limita cu regulile după care pot fi denumite aceste noi malware. Pentru a schimba puțin setarea, subclasele pot fi modificate sau îmbinate împreună, cum ar fi:

Worm.Win64.MSEExcel.RCE.Orice.A

Ceea ce înseamnă că este viermele numit „Whatever”, care infectează sistemele de operare Win64 și folosește RCE (Remote Code Execution) pentru a infecta alte mașini, iar varianta viermelui este prima care este detectată („A”) în sălbăticie.

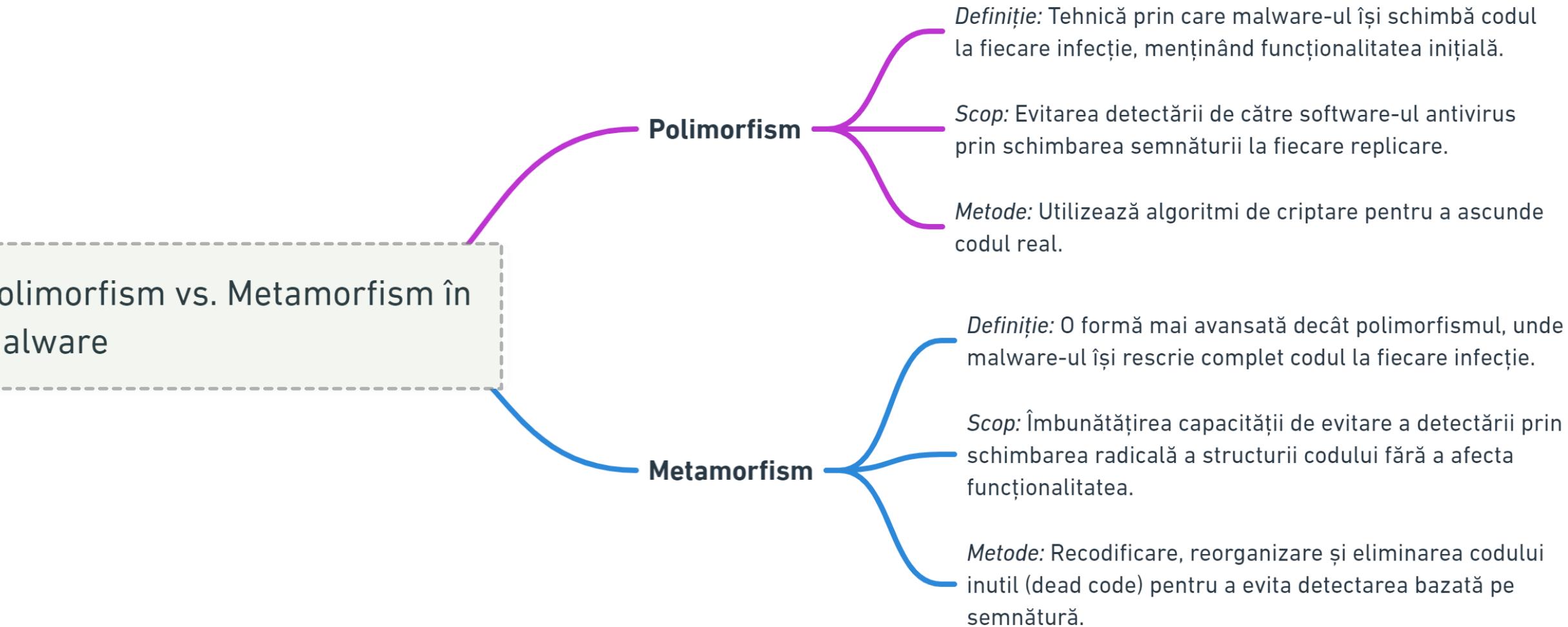
Observați acum că această configurație conține subclase unite (adică OS, FT, AT): Class.[OS][FT][AT].Name.Variant (Tabelul 5). Astfel, acest sistem de notație, deși reducționist, oferă o modalitate structurată de a clasifica și înțelege nenumăratele forme de malware.

C.3.5

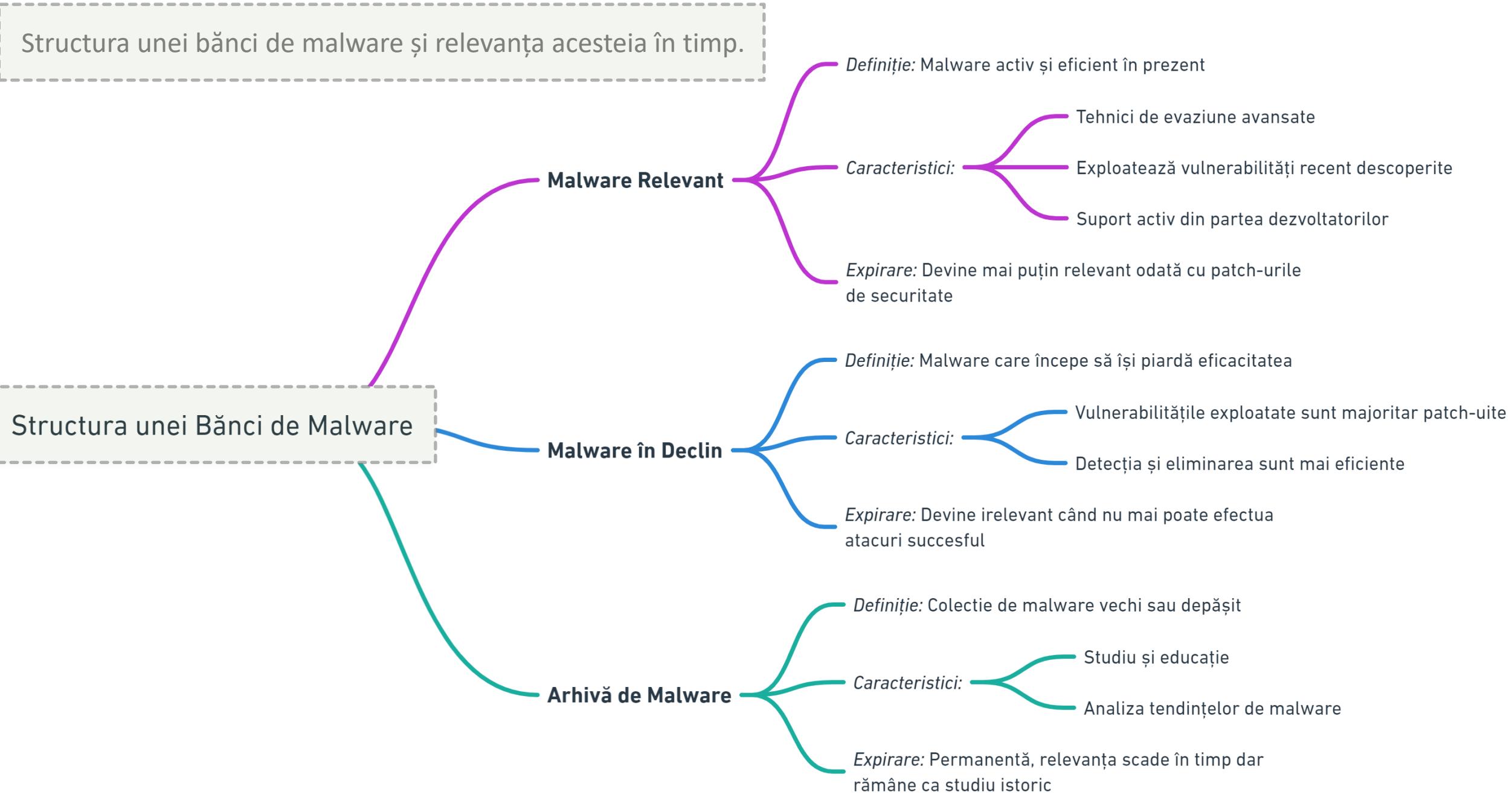
# VALABILITATEA BĂNCII MALWARE SI POLIMORFISM VS METAMORFISM

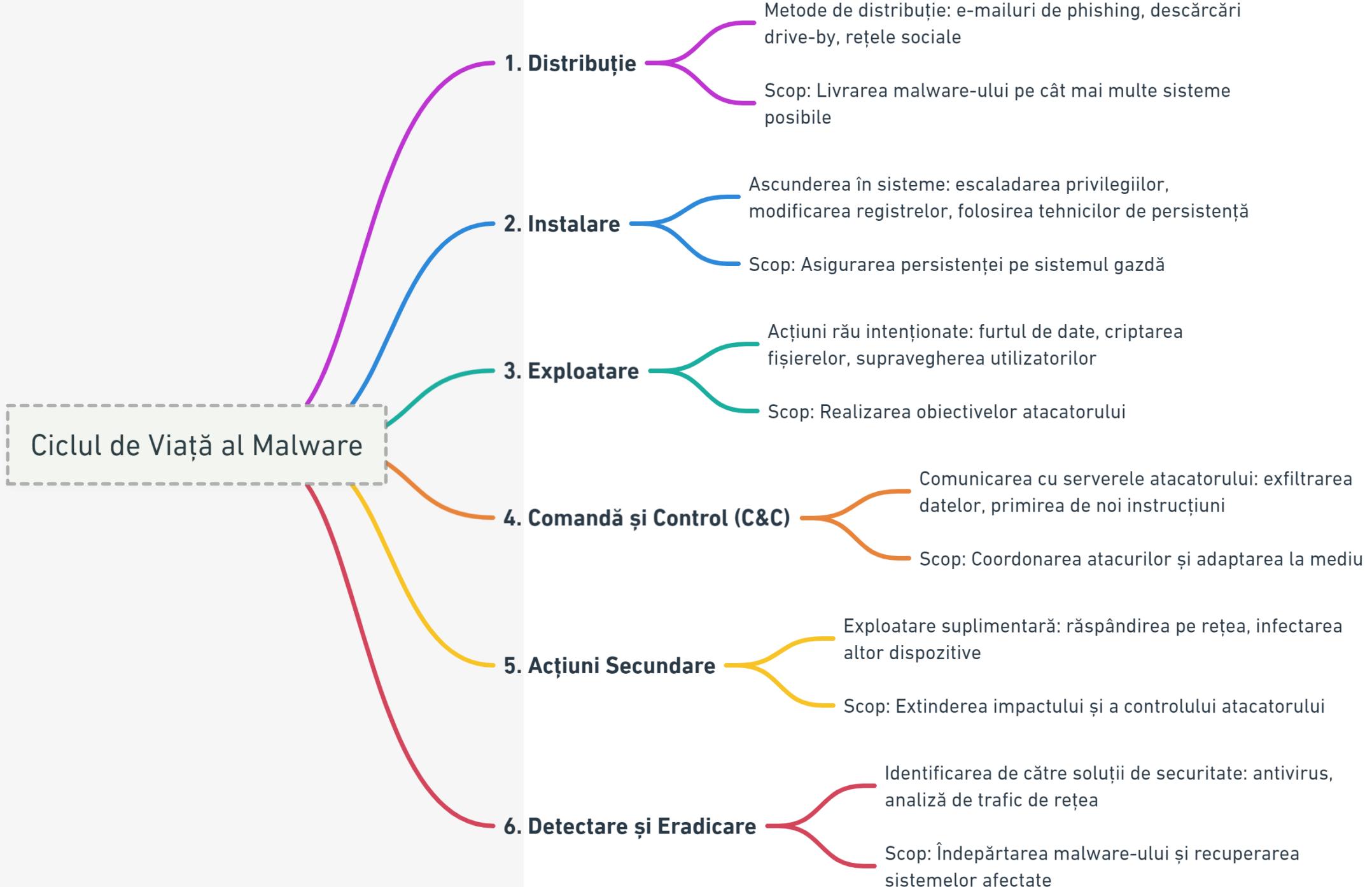


## Polimorfism vs. Metamorfism în Malware



Structura unei bănci de malware și relevanța acesteia în timp.



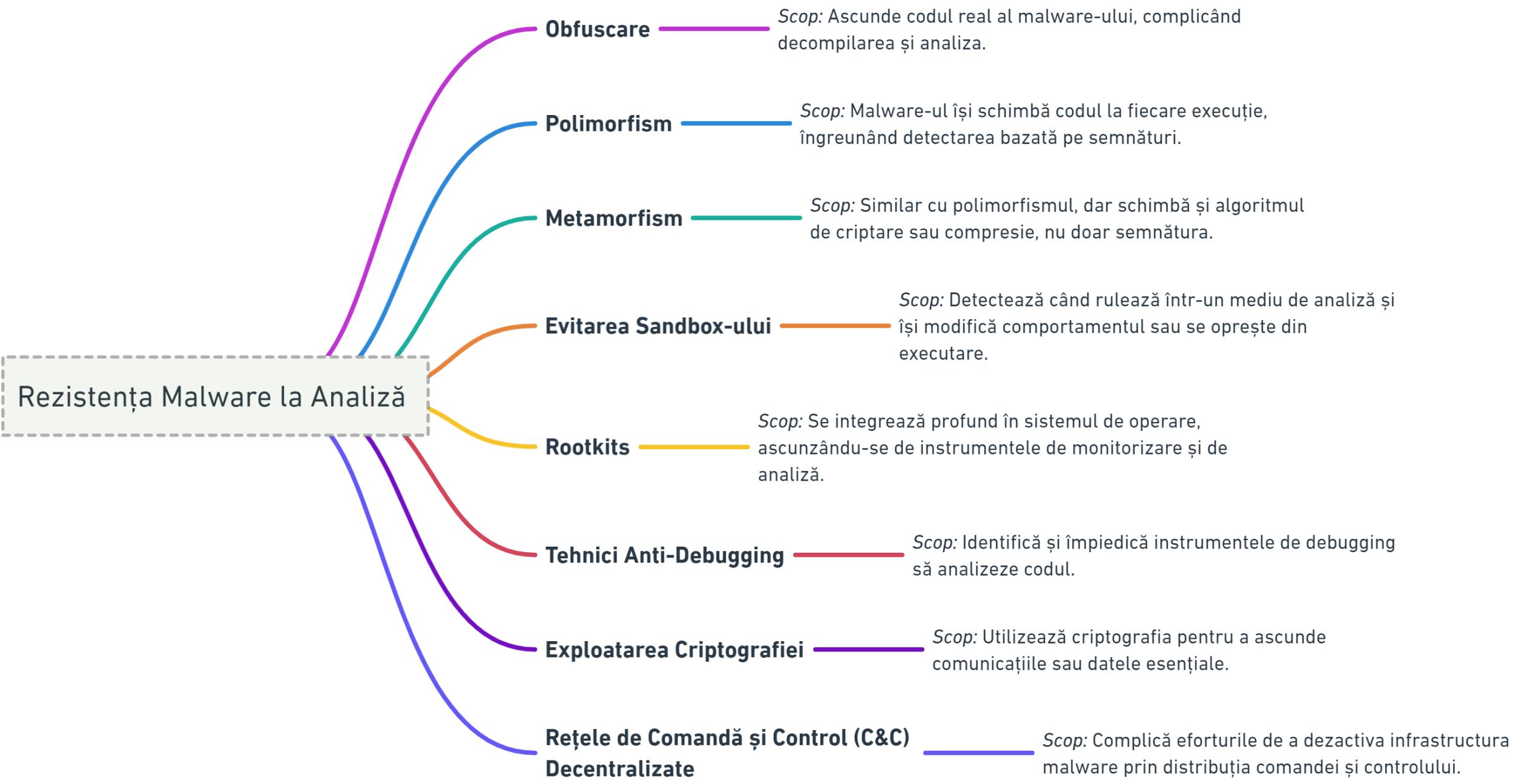


C.3.6

# **CRIPTOGRAFIE, PERSISTENȚĂ, OFUSCARI ȘI EXPLOATĂRI**

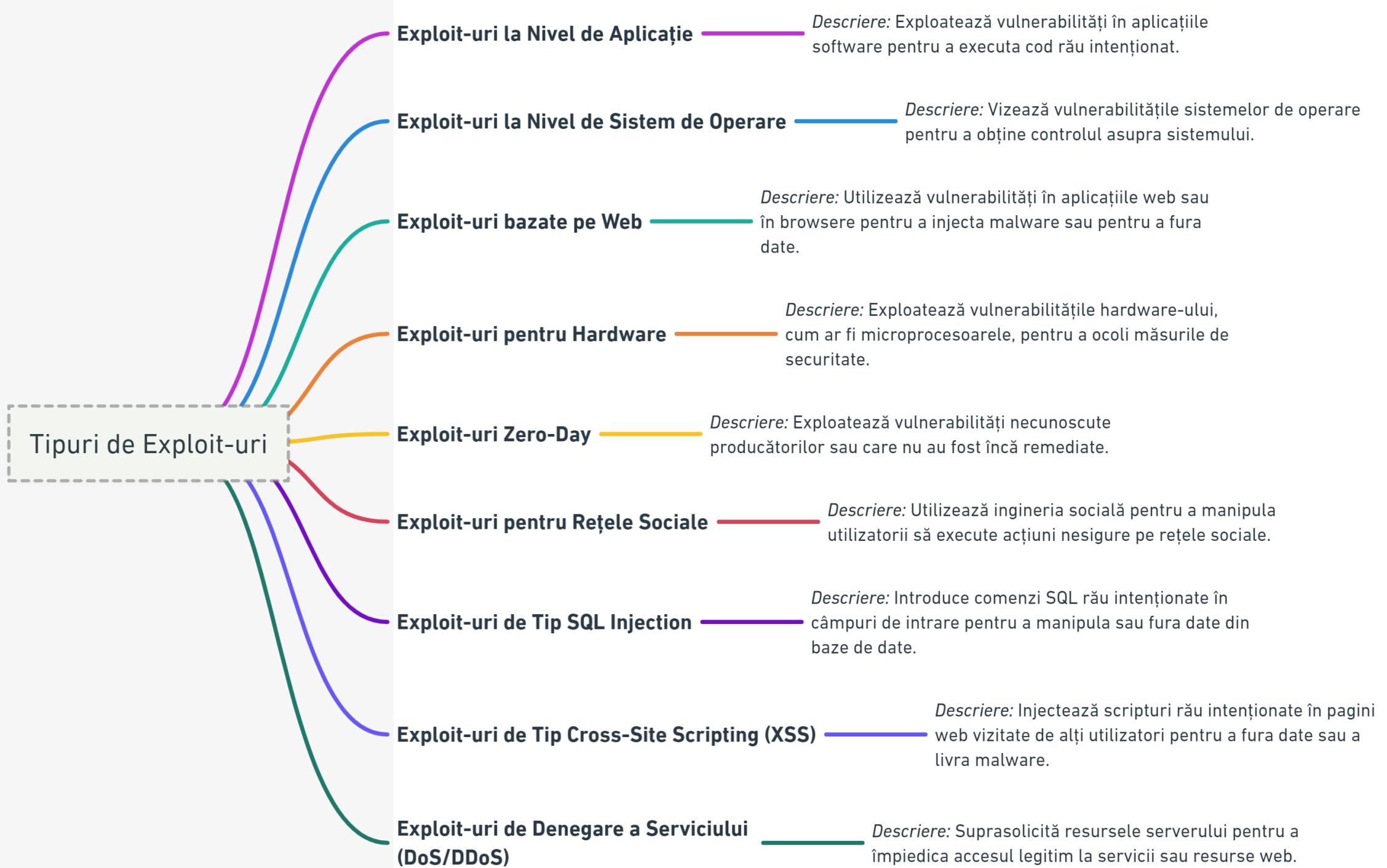






## Tehnici de Ofuscare Folosite În Malware





## Metode de Persistență Utilizate de Malware

- Modificări ale Registrelor** — Descriere: Adăugarea de chei sau valori în registrii Windows pentru a executa malware-ul la pornirea sistemului.
- Scriere în Directorul de Startup** — Descriere: Plasarea de fișiere executabile în directorul de startup al Windows pentru a asigura rularea la fiecare start al sistemului.
- Servicii de Sistem Modificate sau Adăugate** — Descriere: Crearea sau modificarea serviciilor Windows pentru a executa malware-ul ca un serviciu de sistem.
- Planificatorul de Sarcini** — Descriere: Utilizarea Planificatorului de Sarcini Windows pentru a seta execuția malware-ului la anumite intervale de timp.
- Fișiere de Sistem Infectate** — Descriere: Infectarea sau substituirea fișierelor de sistem cu versiuni malware pentru a executa cod rău intenționat.
- Documente Macro Infectate** — Descriere: Exploatarea documentelor cu macro-uri pentru a executa malware-ul atunci când documentul este deschis.
- DLL Hijacking** — Descriere: Explotarea căilor de căutare DLL pentru a încărca biblioteci DLL malware în locul celor legitime.
- Rootkits** — Descriere: Utilizarea rootkits-urilor pentru a ascunde prezența malware-ului și a asigura persistența acestuia, evitând detectarea.

## Criptografia Folosită în Malware

### Criptarea Simetrică

*Descriere:* Cheia de criptare este identică cu cheia de decriptare. Utilizată pentru eficiență în criptarea datelor locale.

*Exemple de Algoritmi:* AES, DES

### Criptarea Asimetrică

*Descriere:* Folosește o pereche de chei: una publică pentru criptare și una privată pentru decriptare. Utilizată în comunicarea securizată între malware și serverul de comandă și control.

*Exemple de Algoritmi:* RSA, ECC

### Steganografia

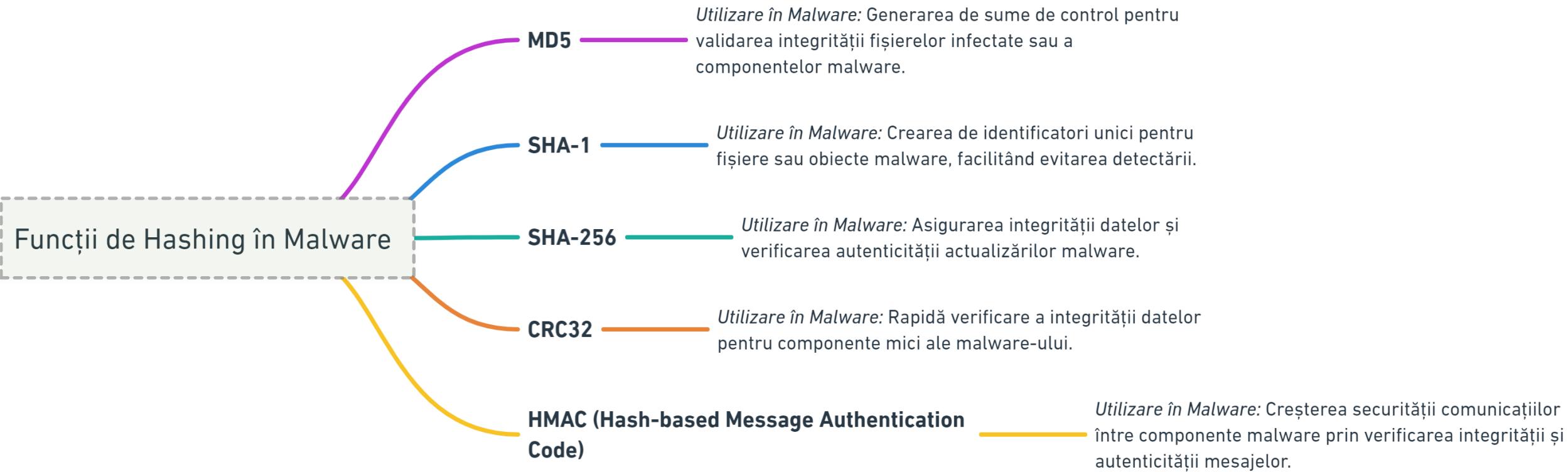
*Descriere:* Ascunderea datelor în cadrul unor fișiere aparent inofensive, pentru a evita detectarea.

*Utilizări Comune:* Transmiterea instrucțiunilor sau actualizațiilor de malware

### Hashing

*Descriere:* Generarea unei valori rezumative dintr-un set de date, utilizată pentru a verifica integritatea datelor sau parolelor fără a le stoca în formă clară.

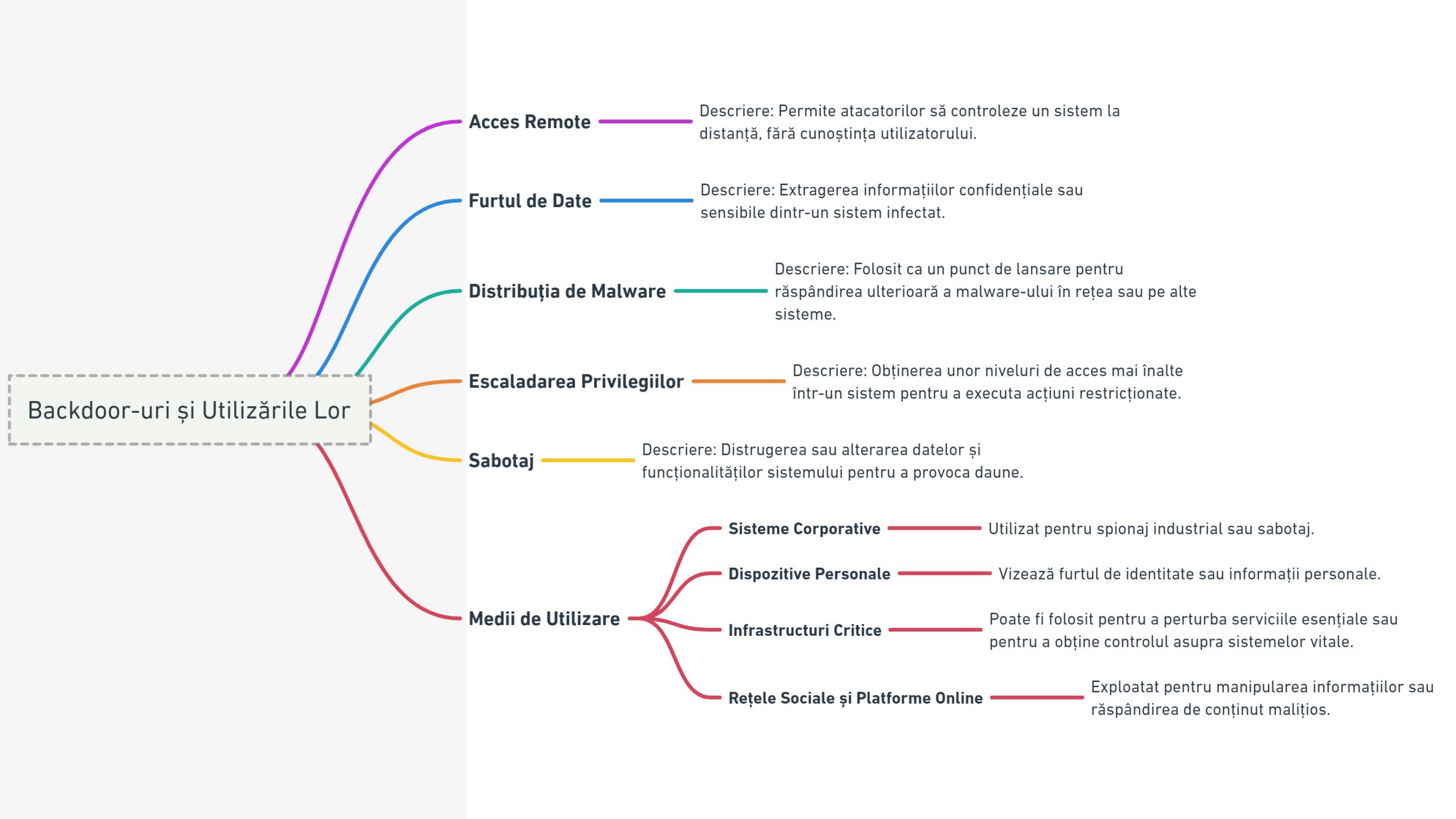
*Exemple de Algoritmi:* SHA-256, MD5

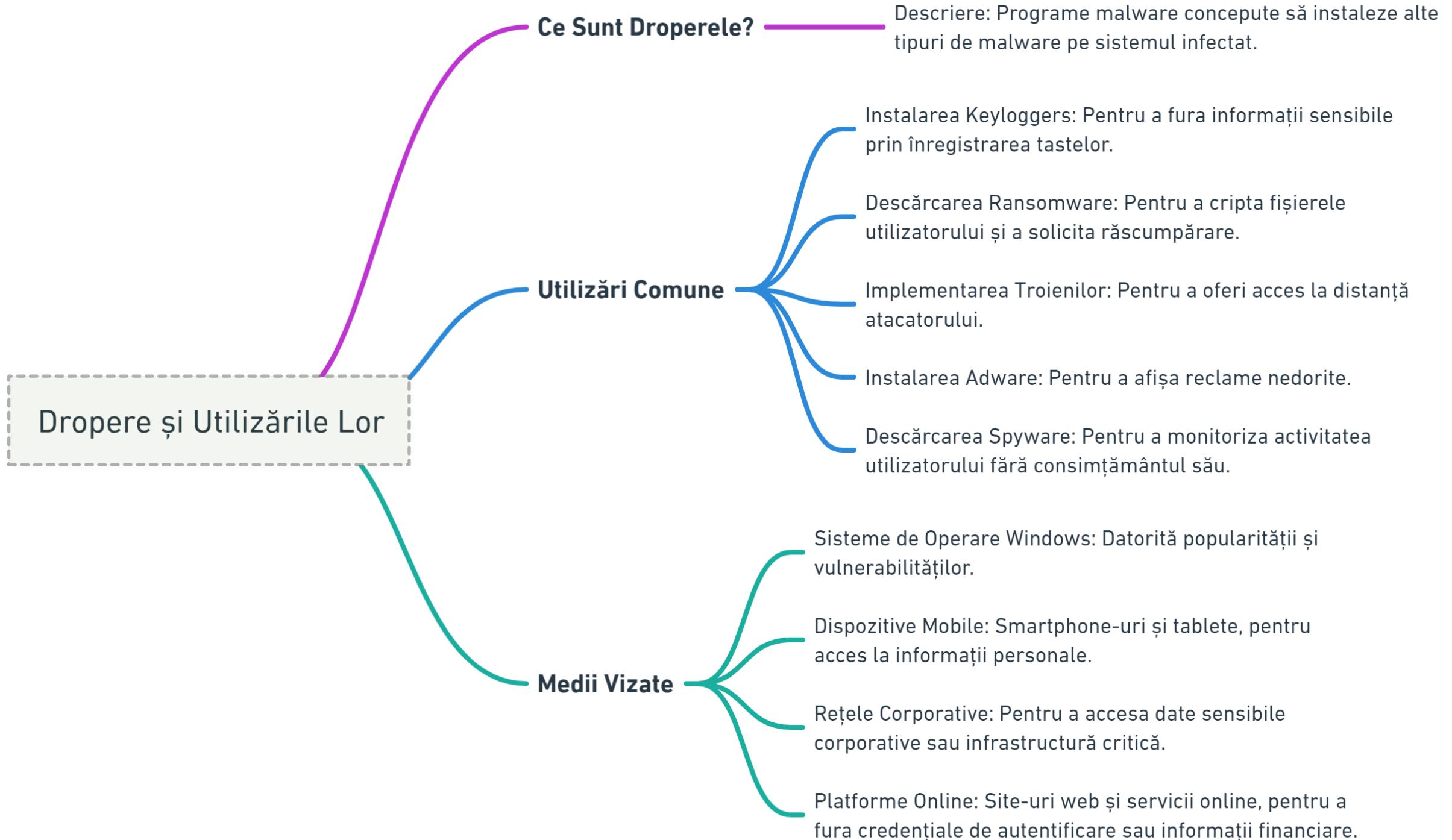


**C.3.7**

# **APLICAȚII DE INFILTRARE: BACKDOOR ȘI DROPPER**





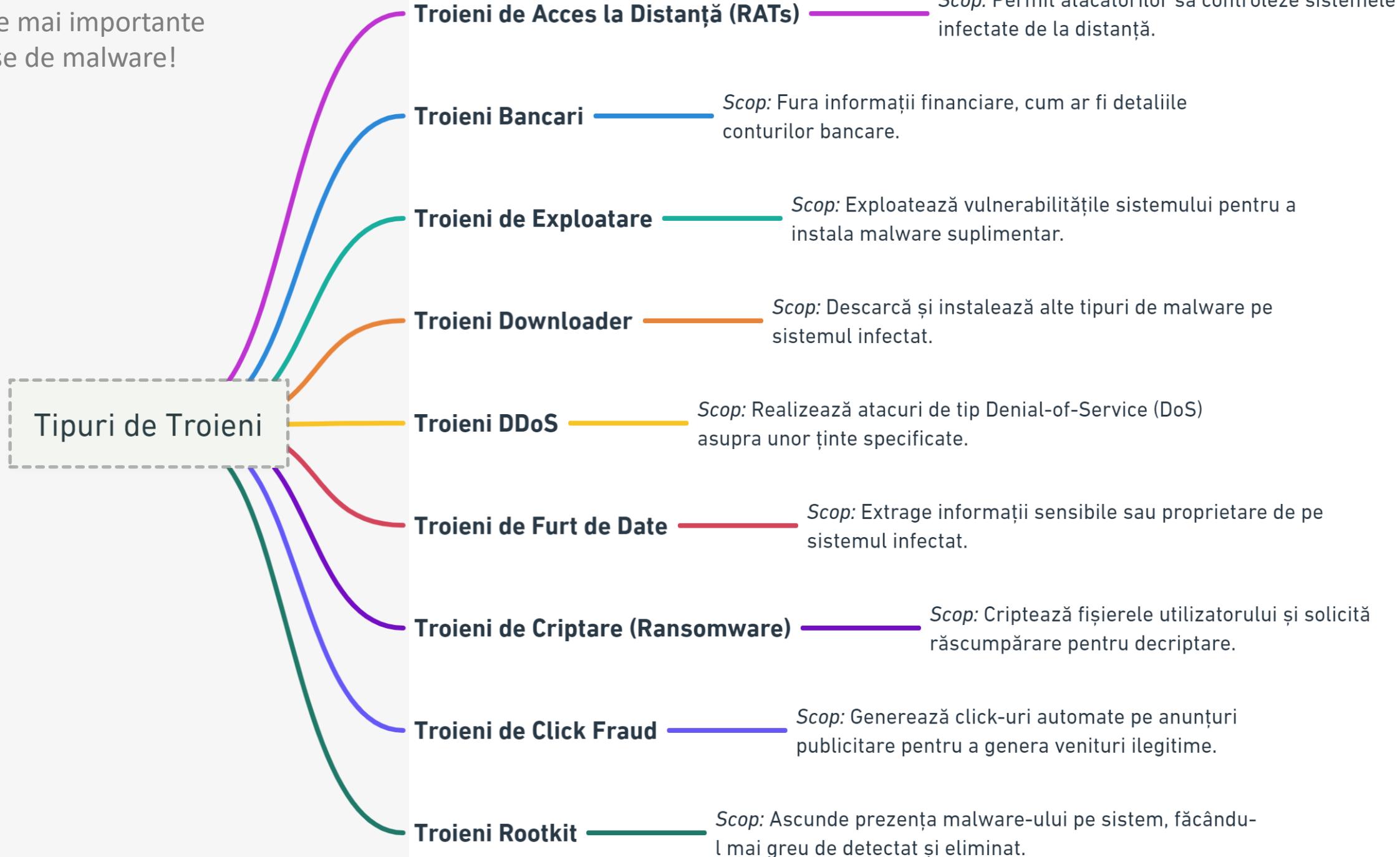


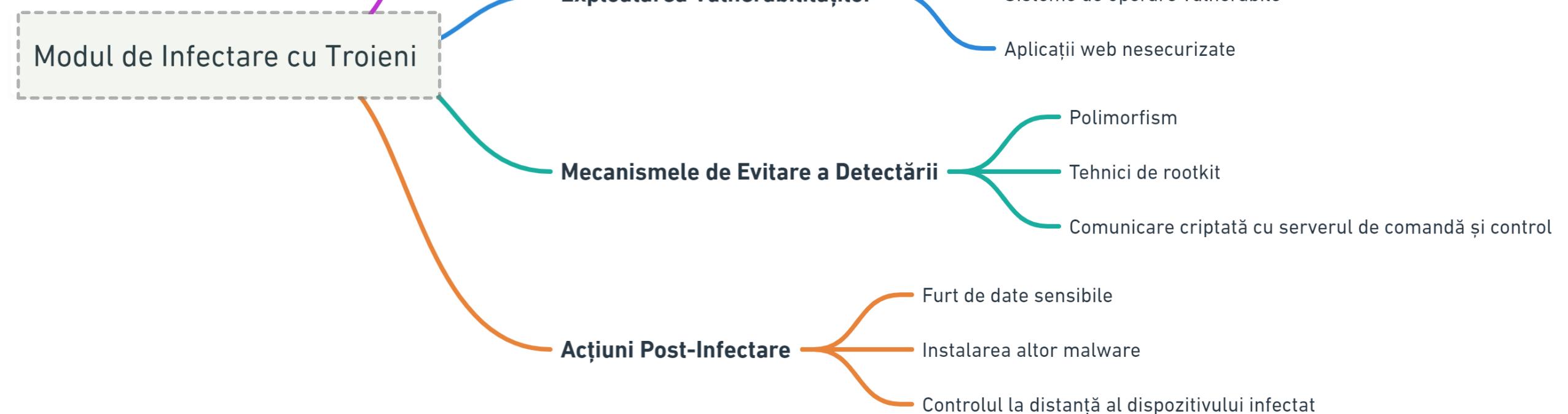
C.3.8

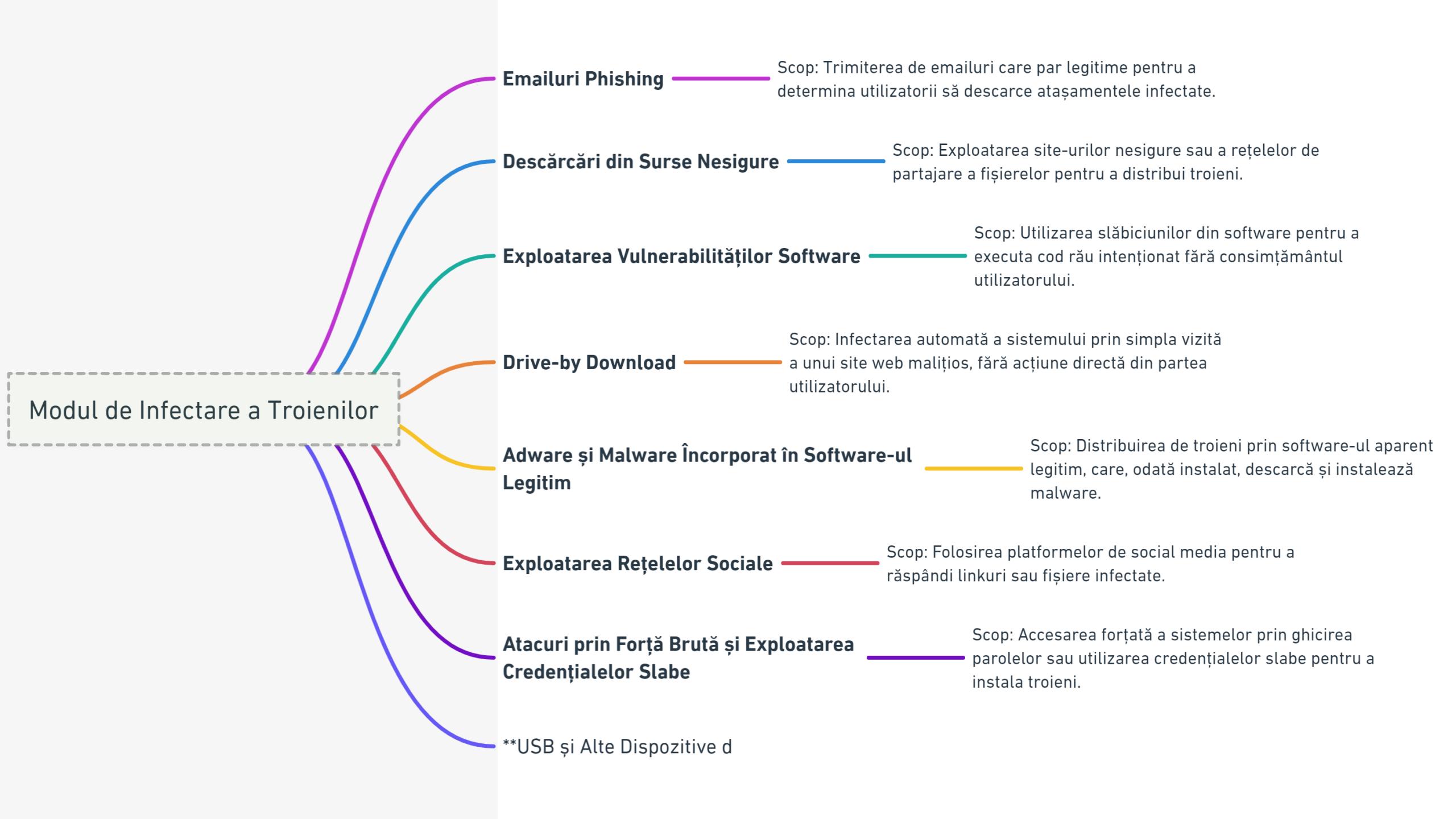
# TIPURI DE TROIENI SI METODELE LOR DE INFECTARE



Cele mai importante clase de malware!







c.3.9

# TIPURI DE VIERMI ȘI METODELE LOR DE INFECTARE



## Cele mai importante clase de malware!

### Tipuri de Wormi

#### Wormi de Email

Exploatează sistemele de email pentru a se auto-răspândi trimînd copii ale lor către adresele din lista de contacte a victimei.

#### Wormi de Rețea

Exploatează vulnerabilitățile din software-ul de rețea pentru a se răspândi automat între computere conectate la aceeași rețea.

#### Wormi de Internet

Utilizează vulnerabilitățile de pe internet pentru a infecta computere la nivel global, adesea fără interacțiunea utilizatorului.

#### Wormi de Instant Messaging

Răspândirea se face prin mesaje automate trimise prin aplicații de mesagerie instant, care conțin link-uri sau fișiere infectate.

#### Wormi File-sharing

Se răspândesc prin rețele de partajare a fișierelor, infectând fișiere care sunt apoi descărcate și executate de alții utilizatori.

#### Wormi Multipartiți

Combină metodele de infectare ale diferitelor tipuri de wormi pentru a-și maximiza răspândirea și eficacitatea.

## Mecanismele de Infectie ale Wormilor (Viermilor)

### Exploatarea Vulnerabilităților de Software

Scop: Utilizarea slăbiciunilor din software pentru a executa cod rău intenționat fără interacțiune umană.

### Emailuri Infectate

Scop: Trimiterea de emailuri cu atașamente sau linkuri malicioase către victime pentru a răspândi malware-ul.

### Rețele Sociale și Mesagerie

Scop: Răspândirea prin mesaje malicioase sau linkuri posteate pe rețele sociale sau prin aplicații de mesagerie.

### Drive USB Infectate

Scop: Infectarea calculatoarelor prin conectarea de dispozitive de stocare USB care conțin malware.

### Rețele Peer-to-Peer (P2P)

Scop: Distribuirea worm-ilor prin fișiere partajate pe rețele P2P, mascate ca software legitim sau fișiere multimedia.

### Servicii de File Sharing

Scop: Explotarea serviciilor de partajare a fișierelor pentru a răspândi malware-ul prin fișiere infectate descărcate de victime.

### Site-uri Web Compromise

Scop: Infectarea vizitorilor prin vulnerabilități web sau prin descărări malicioase ascunse pe site-uri compromise.

C.3.10

# TIPURI DE VIRUȘI, CICLUL LOR DE VIAȚĂ ȘI METODE DE INFECTARE



Cele mai importante clase de malware!

## Tipuri de Viruși Informatici

- Virusi de Boot Sector** Scop: Infectarea sectorului de boot al unui dispozitiv de stocare pentru a se executa înaintea sistemului de operare.
- Virusi de Macro** Scop: Exploatarea macro-urilor din documentele Microsoft Office pentru a executa cod rău intenționat.
- Virusi Polimorfici** Scop: Modificarea propriului cod la fiecare infecție pentru a evita detectarea de către software-urile antivirus.
- Virusi Metamorfici** Scop: Rescrierea completă a propriului cod la fiecare infecție, făcându-i și mai greu de detectat.
- Virusi de Fisiere** Scop: Atașarea sau inserarea în fișiere executabile pentru a se executa odată cu acestea.
- Virusi de Retea** Scop: Explotarea vulnerabilităților rețelei pentru a se răspândi fără a fi nevoie de interacțiune umană.
- Virusi de Email** Scop: Răspândirea prin atașamente de email infectate sau prin linkuri rău intenționate.
- Troieni** Scop: Maschează ca software legitim pentru a executa acțiuni rău intenționate fără știrea utilizatorului.
- Worms** Scop: Auto-replicarea și răspândirea în rețele pentru a infecta cât mai multe dispozitive posibil.

## Tipuri de Viruși Informatici

### Virus de Boot Sector

Descriere: Infectează sectorul de boot al dispozitivelor de stocare, executându-se la pornirea sistemului.

### Virus de Fișier sau Program

Descriere: Se atașează de fișiere executabile sau programe, infectându-le atunci când sunt executate.

### Macro Virus

Descriere: Se răspândește prin documente care conțin macrocomenzi, cum ar fi documentele Microsoft Office.

### Virus Polimorfic

Descriere: Își schimbă codul (semnătura) la fiecare infecție, făcându-l dificil de detectat de programele antivirus.

### Virus Metamorfic

Descriere: Se rescrie complet la fiecare infecție, pentru a evita detectarea, păstrându-și funcționalitatea.

### Virus Companion

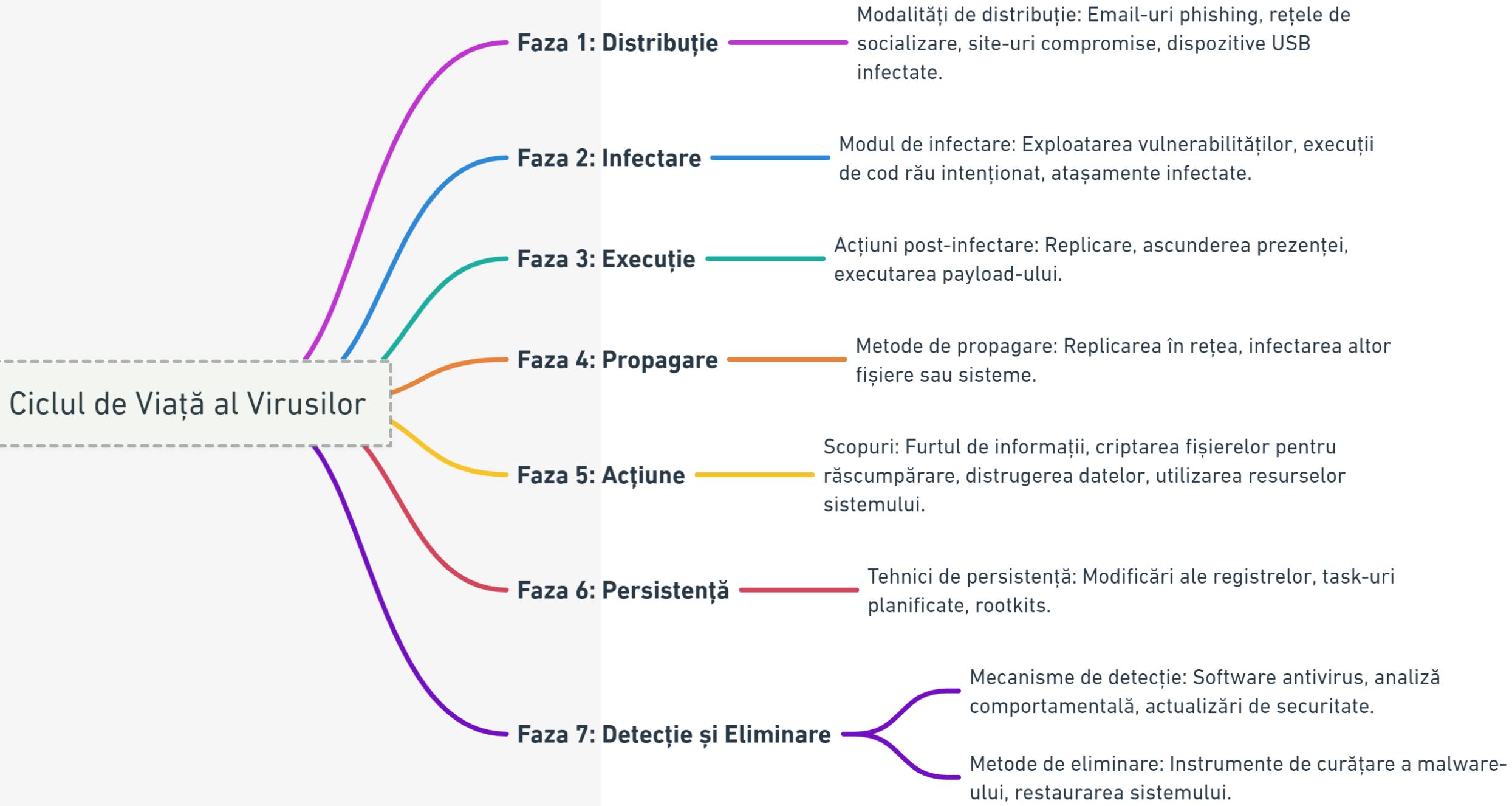
Descriere: Creează un fișier companion pentru fișierele executabile existente; când fișierul original este executat, virusul este de asemenea lansat.

### Virus de Script

Descriere: Se răspândește prin scripturi rulabile, cum ar fi cele din paginile web sau e-mailuri.

## Virusi de Tip Infector de Fișier

- 
- Virus Direct** — *Descriere: Infectează direct fișierele executabile, modificându-le pentru a include codul virusului.*
  - Virus de Supraîncărcare (Overwriting)** — *Descriere: Înlocuiește conținutul fișierului original cu codul virusului, distrugând astfel informația inițială.*
  - Virus de Prepending** — *Descriere: Adaugă codul virusului la începutul fișierului infectat, executându-se înaintea codului original al fișierului.*
  - Virus deAppending** — *Descriere: Adaugă codul virusului la sfârșitul fișierului, modificând punctul de intrare al programului pentru a executa mai întâi virusul.*
  - Virus de Companion** — *Descriere: Creează un nou fișier care este executat în locul unuia original, redirecționând execuția spre virus.*
  - Virus Linker** — *Descriere: Modifică referințele la fișiere executabile pentru a executa virusul înainte de fișierul original.*



# 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>

