Cele 25 de clase de malware din datasetul Malimg

**🛑 Dialere (Dialer)**

1. **Adialer.C** – Un program care folosește modemul pentru a apela numere cu tarif special, generând costuri suplimentare pentru utilizator. ([Microsoft](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Dialer%3AWin32%2FAdialer.C&utm_source=chatgpt.com))
2. **Dialplatform.B** – Similar cu Adialer.C, utilizează modemul pentru a apela numere cu tarif premium, afectând utilizatorii cu conexiuni dial-up. ([Microsoft](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Dialer%3AWin32%2FDialPlatform.B&utm_source=chatgpt.com))
3. **Instantaccess** – Un dialer care conectează utilizatorul la servicii cu conținut pentru adulți prin apeluri la numere cu tarif special și poate instala suplimentar alte programe malițioase. ([Microsoft](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Dialer%3AWin32%2FInstantAccess&utm_source=chatgpt.com))

**🧬 Viermi și Răspândire în Rețea**

1. **Allaple.A & Allaple.L** – Viermi de rețea polimorfici care se răspândesc prin rețele LAN și pot lansa atacuri de tip DoS. ([Microsoft](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32%2FAllaple&utm_source=chatgpt.com))
2. **Autorun.K** – Malware care se răspândește prin dispozitive amovibile, folosind fișierul autorun.inf pentru a se executa automat la conectarea dispozitivului. ([Microsoft Answers](https://answers.microsoft.com/en-us/windows/forum/all/autorun-virus-removal/991677c0-a10c-4bf0-9fe4-47b5f989a646?utm_source=chatgpt.com))

**🕵️‍♂️ Troieni și Rootkit-uri**

1. **Alueron.gen!J** – Troian și rootkit care interceptează traficul de rețea pentru a fura date sensibile, precum informații bancare. ([Wikipedia](https://en.wikipedia.org/wiki/Alureon?utm_source=chatgpt.com" \o "Alureon - Wikipedia))
2. **C2LOP.P & C2LOP.gen!g** – Troieni care modifică setările browserului, adaugă semne de carte către site-uri publicitare și afișează reclame pop-up. ([Microsoft](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FC2Lop&utm_source=chatgpt.com))
3. **Dontovo.A** – Troian downloader care descarcă și execută alte programe malițioase pe sistemul infectat. ([F-Secure](https://www.f-secure.com/v-descs/trojan-downloader-w32-fakerean-gen%21a.shtml?utm_source=chatgpt.com))
4. **Fakerean** – Program antivirus fals care afișează alerte înșelătoare pentru a convinge utilizatorul să achiziționeze o licență inutilă.
5. **Malex.gen!J** – Troian generic care poate descărca și executa fișiere malițioase suplimentare.
6. **Obfuscator.AD** – Malware care utilizează tehnici de ofuscare pentru a evita detectarea de către software-ul antivirus.([F-Secure](https://www.f-secure.com/v-descs/trojan-downloader-w32-fakerean-gen%21a.shtml?utm_source=chatgpt.com))
7. **Rbot!gen** – Troian care transformă sistemul infectat într-un bot controlat de la distanță, permițând atacuri de tip DDoS sau furt de informații.
8. **Skintrim.N** – Malware care modifică interfața utilizatorului sau comportamentul sistemului pentru a induce în eroare utilizatorul.
9. **Swizzor.gen!E & Swizzor.gen!I** – Troieni care descarcă și execută fișiere malițioase suplimentare, adesea utilizate pentru a instala adware sau alte tipuri de malware.
10. **VB.AT** – Troian scris în Visual Basic, utilizat pentru a executa comenzi malițioase pe sistemul infectat.
11. **Wintrim.BX** – Malware care poate modifica setările sistemului sau instala programe nedorite fără consimțământul utilizatorului.
12. **Yuner.A** – Troian care poate deschide porturi de rețea pentru a permite accesul neautorizat la sistemul infectat.

**🔐 Furt de Informații**

1. **Lolyda.AA1, AA2, AA3 & AT** – Troieni care fură informații sensibile, în special date de autentificare pentru jocuri online, și le trimit către atacatori.

Dacă ai nevoie de informații suplimentare despre oricare dintre aceste clase de malware sau despre metode de protecție împotriva acestora, nu ezita să întrebi!

## Boosting

**Boosting** este o tehnică de învățare automată de tip **ensemble** în care mai multe modele slabe (weak learners) — de obicei arbori de decizie simpli — sunt antrenate **secvențial**, fiecare încercând să corecteze greșelile făcute de modelele anterioare.

**🌟 Ce este *Gradient Boosting*?**

Este o formă specifică de boosting în care fiecare nou model este antrenat pentru a **reduce eroarea (residuala)** a modelului anterior, folosind **gradientul** unei funcții de pierdere (loss function).

**🔄 Cum funcționează:**

1. **Se antrenează un model slab** (ex: un arbore mic) pe datele originale.
2. Se calculează **eroarea** dintre predicțiile lui și valorile reale.
3. Se construiește **un nou model** care învață să prezică această eroare (adică gradientul funcției de pierdere).
4. Se adună predicțiile modelului nou la predicțiile vechi.
5. Se repetă procesul (de obicei de câteva zeci sau sute de ori).

**🧠 Intuiție:**

Imaginează-ți că în fiecare pas încerci să "repari" greșelile făcute anterior. Cu fiecare model adăugat, te apropii din ce în ce mai mult de răspunsul corect.

**📌 Exemplu simplificat:**

from sklearn.ensemble import GradientBoostingClassifier

model = GradientBoostingClassifier(n\_estimators=100, learning\_rate=0.1, max\_depth=3)

model.fit(X\_train, y\_train)

* n\_estimators: câți arbori slabi sunt în lanț
* learning\_rate: cât de mult corectează fiecare model greșelile anterioare
* max\_depth: cât de complex este fiecare arbore (de obicei mic, ex: 3)

**✅ Avantaje:**

* Funcționează foarte bine pe multe tipuri de date.
* Oferă rezultate competitive în concursuri de tip Kaggle.
* Poate modela relații complexe nelineare.

**❗️Dezavantaje:**

* Timp de antrenare mai lung.
* Sensibil la date zgomotoase dacă nu e reglat bine (risc de overfitting).
* Mai greu de interpretat decât un model simplu.

Vrei să-ți explic și diferența dintre **bagging** și **boosting** sau să vezi cum funcționează XGBoost, care e o versiune optimizată?