



ROMÂNIA SUB ATAC :

EȘTI PREGĂTIT SAU
EȘTI URMĂTORUL?



HARTA ATACURILOR

- 217 atacuri documentate în presa din România
- Amenzi GDPR • Cazuri reale • 2020-2026



217

Atacuri
România

105

Instituții
publice

112

Companii
private

41

Județe
afectate

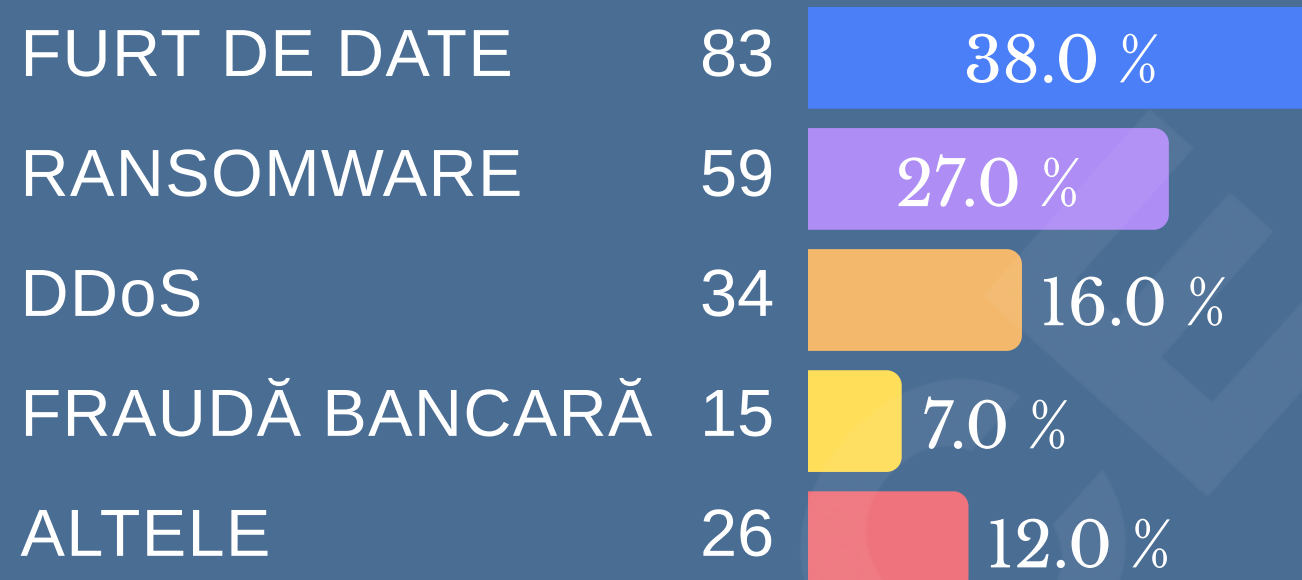


TIPOLOGIA ATACURILOR

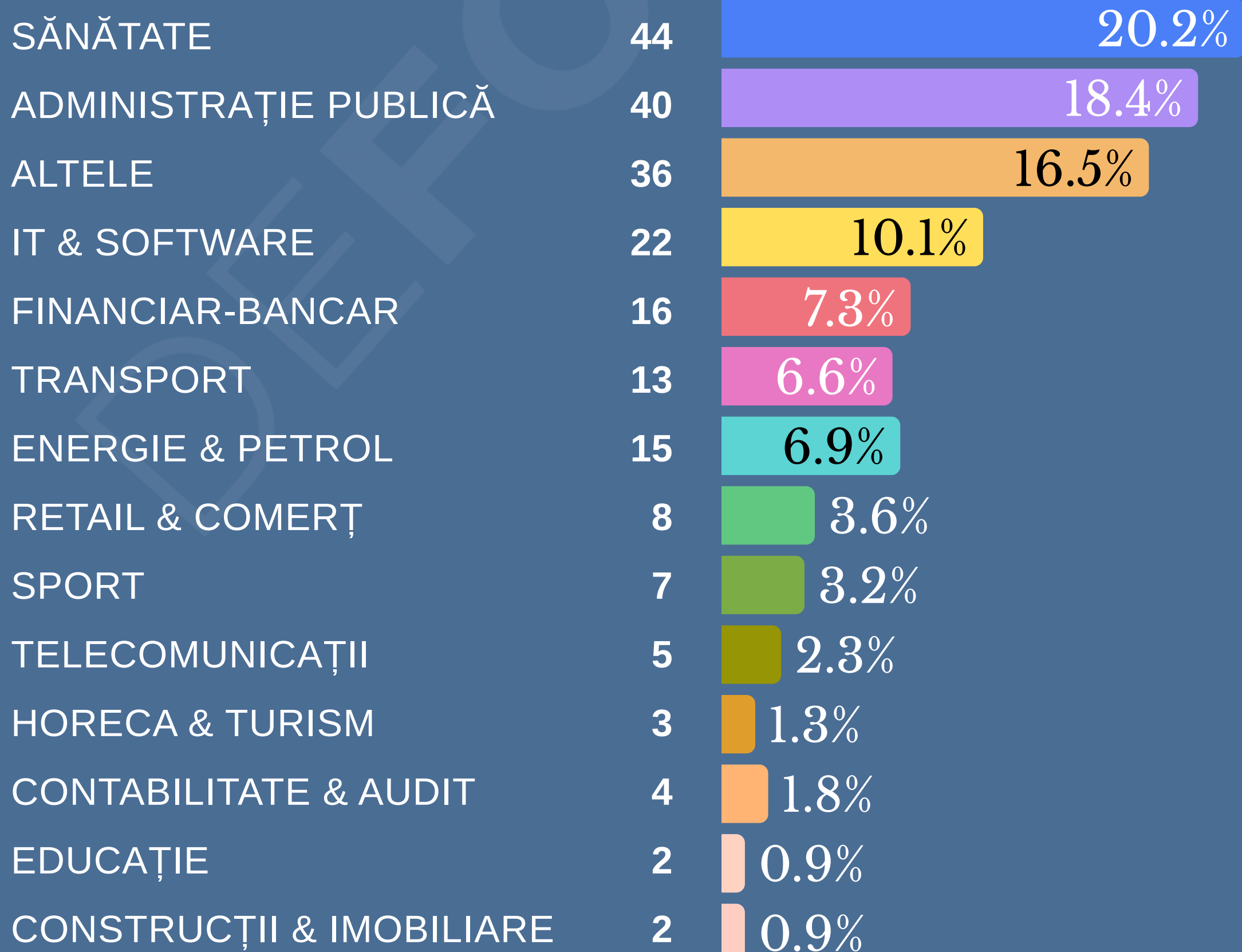
- 217 incidente analizate • Date combinate din presa română
- Actualizat Mai 2026



TIP ATAC



SECTOR ACTIVITATE



CAZURI REALE

- Cele mai grave atacuri documentate în presa din România

#1

26 SPITALE - O SINGURĂ NOAPTE

RANSOMWARE

- Sistemul Hipocrate (RSC) - Feb. 2024

În noaptea de 11–12 februarie 2024, un atac ransomware Backmydata/Phobos a afectat cel puțin 26 de spitale din România, criptând sistemele platformei Hipocrate și blocând accesul la date medicale. Atacatorii au cerut 3,5 BTC (~157.000 EUR), iar incidentul este investigat de DNSC și DIICOT.

#2

APELE ROMANE - 1.000 DE SISTEME BLOCATE

RANSOMWARE

- ANAR - Dec. 2025

Apele Române au fost lovite în decembrie 2025 de un atac ransomware care a compromis aproximativ 1.000 de sisteme IT, inclusiv servere și baze de date. Atacatorii au folosit BitLocker pentru a cripta datele și au transmis o notă de răscumpărare. Infrastructura operațională nu a fost afectată, iar incidentul este investigat de DNSC și SRI.

#3

RENAULT - RECORD AMENDĂ GDPR

FURT DE DATE

- Mar. 2026

Renault Commercial Roumanie a fost sancționată cu 125.000 EUR după un atac cibernetic asupra unei aplicații administrate de un împuternicit, care a dus la publicarea online a unui volum mare de date personale (inclusiv CNP, acte de identitate și date de contact). ANSPDCP a constatat lipsa măsurilor adecvate de securitate și nerespectarea obligațiilor privind împuterniciții.

CAZURI REALE

- Cele mai grave atacuri documentate în presa din România

#4 MEDICI BIHOR - 1 MILION DE LEI FURAȚI

FRAUDE BANCARE

• Feb 2025

Mai mulți medici de familie din Bihor au fost victimele unor atacuri de inginerie socială între 3–14 februarie 2025, în care atacatorii, pretinzând că sunt reprezentanți ai Bursei de Valori București, au determinat instalarea unor aplicații de control la distanță și au compromis conturile bancare ale victimelor, generând pagube de sute de mii de euro.

#5 BCR + ALPHA BANK + BANCA TRANSILVANIA

DDOS

• Mar. 2024

O grupare pro-rusă (NoName75) a lansat un atac DDoS asupra BCR, Banca Transilvania și Alpha Bank pe 15 martie 2024, provocând disfuncționalități temporare ale serviciilor online. Băncile au blocat traficul malițios, iar datele și conturile clienților nu au fost afectate.

Realitatea unui atac, fără filtre

- Ce se întâmplă concret când ești lovit

1 PIERDERI FINANCIARE DIRECTE

Fonduri transferate în conturi ale atacatorilor, răscumpărări plătite, costuri de recuperare.

Medici Bihor: ~1M lei • FCSB/COMAN: 6,25m EUR • Camera Dep: 40K EUR cerut

2 AMENZI GDPR - CHIAR DACĂ EȘTI VICTIMĂ

ANSPDCP nu te întreabă dacă ai știut. Te întreabă dacă ai luat măsuri. Răspunsul „am fost atacat” nu te scutește de amendă.

Renault: 125.000 EUR • EON: 25.000 EUR • NTT Data: 25.000 EUR

3 OPRIREA COMPLETĂ A ACTIVITĂȚII

Nu pierzi doar date. Pierzi zile, clienți și contracte. Fiecare oră de inactivitate are un cost real — înainte să plătești un leu pentru recuperare.

Recuperarea durează în media 1-3 săptămâni. Unele organizații au pierdut date definitiv

4 REPUTAȚIE DISTRUSĂ

Știrea rămâne pe Google pentru totdeauna. Încrederea clienților — nu se mai întoarce la fel.

Altex / Orange / Vodafone / Bitdefender - toate au știri negative în presa națională

5 DOSAR PENAL

Amenda GDPR e doar începutul. Dacă vulnerabilitățile erau cunoscute și ignorate, urmează parchetul. Director IT, CEO, administrator — toți pot răspunde penal.

DIICOT intrumentează dosare. CONPET: dosar penal deschis după atac (Feb 2026)



AMENZI GDPR

- A fi victimă a unui atac NU te scutește de amendă. ANSPDCP sancționează lipsa măsurilor de securitate



Total amenzi documentate: 459.000 Euro

LISTĂ SURSĂ ATACURI

- SRI a contribuit la stoparea unor atacuri cibernetice (APT28/GRU)
- Escrocherie prin Microsoft Teams — malware ModeloRAT infectează rețele corporative
- Escrocherie WhatsApp — „Bună tată, sunt eu” — cum rămân părinții fără bani
- Hackeri asociați Chinei infiltrează rețele telecom din România cu malware BPFDoor
- Un nou val de fraudă online folosind identitatea vizuală a presei și persoanelor publice
- Site-ul ISJ Bihor a fost spart — mesajul hackerului D3v1X
- Lupta cu hackerii — Primăria Oradea, al doilea atac masiv: sute de calculatoare criptate
- Hackerii Kremlinului au spart zeci de conturi ale Forțelor Aeriene Române, inclusiv de la baze NATO
- Cum a creat haos în Ungaria un hacker de 17 ani din Bihor — operațiune antitero bilaterală
- DIICOT Oradea — fraudare aparate jocuri de noroc, instrumente de plată falsificate (Bihor/Maramureș)
- DIICOT Oradea — grup infracțional CAS Bihor: fraudă informatică, consultații fictive, 2,4M lei prejudiciu
- Percheziții la două doctorițe din Bihor — prescripții electronice false în sistemul CNAS
- Comunicat DIICOT — forum Darkode destructurat, membri români implicați
- Hackerul orădean Guccifer — eliberat după aproape 8 ani de închisoare, și-a spart memoriile
- O grupare de falsificatori de carduri condusă de un orădean a scos peste 600.000 EUR din conturi americane
- Atac cibernetice — Realitatea, RLive TV — 250.000 tentative în 21 de zile
- Click, te-am țepuit! Fraudele cu troieni bancari asupra companiilor bihorene
- România, țintă a atacurilor cibernetice — Radu Miruță: peste 10.000 de atacuri
- Fraudă cu apeluri telefonice false în numele Poliției și BNR

LISTĂ SURSĂ ATACURI

- Atac cibernetic asupra unei firme de contabilitate din Oradea — hackerii au cerut recompensă de mii de euro
- Jucătorii de Minecraft, ținta unui malware care fură date personale
- Pachete oficiale SAP compromise într-un atac asupra lanțului de aprovizionare software
- Atac cibernetic la o firmă de asigurări din Oradea — date sensibile expuse, amendă 5.000 EUR (AG Broker)
- Gruparea Lazarus Group vizează utilizatori macOS din România prin tehnica ClickFix
- Atac cibernetic asupra Electrica Distribuție Transilvania — peste un milion de clienți în pericol
- Dacia Mioveni, afectată de atacul informatic WannaCry
- Bogdan Ivan — atac cibernetic masiv asupra site-ului DNSC, 18.000 accesări/secundă
- Ce este frauda SIM Swap în online banking și cum se previne
- Fraudă online cu amenzi de circulație false — alertă DNSC: nu accesați link-urile
- EMA/ANMMDMR România — documente vaccin Pfizer/BioNTech furate de gruparea Maze
- Un nou val de atacuri — email fals de la firmă de avocatură, malware extrage cookie-uri și tokenuri
- Lapsus revendică un nou atac asupra Vodafone România — cod sursă furat din GitHub
- SMS-uri cu amenzi rutiere false trimise în numele sistemului e-Sigur — cum te protejezi
- Poliția din Viena a reținut o bandă de escroci
- DNSC — avertisment privind fraudele care folosesc imaginea Loteriei Române
- Un român a spart sistemul informatic al unei bănci din Islanda
- Un atac de tip supply chain a compromis biblioteca populară Axios
- O rețea folosită la ascunderea adresei de internet a infractorilor



LISTĂ SURSĂ ATACURI

- Campanie de spionaj desfășurată la nivel global de Rusia, descoperită de FBI
- Atac DDoS — Portalul ghiseul.ro
- Atac cibernetic — Website-ul Facultății de Științe Economice
- Atac cibernetic — CONPET S.A. Sistemul Național de Transport
- Atac ransomware — Spitalul de Pneumoftiziologie și Boli Infecțioase Brașov
- Fraudă bancară — Persoane fizice înșelate prin metoda „curierului”
- Atac cibernetic — DIICOT, Eurojust și Europol
- Atac cibernetic — Ledger, portofelul crypto
- Furt de date — Under Armour
- Furt de date — Site-urile Uniunii Europene
- Furt de date — Dezvoltator de software
- Furt de date — BLUE PROJECTS S.R.L. — Amendă 2.500 EUR
- Atac DDoS — Conpet
- Atac DDoS — Atac cibernetic asupra MAE
- Atac cibernetic — ANAF
- Atac DDoS — Site-ul Digi24.ro a fost clonat
- Furt de date — PREMIER RESTAURANTS ROMANIA SRL — Amendă 8.000 EUR
- Acces neautorizat — Site-ul Camerei Deputaților
- Atac DDoS — Platformele eviza.mae.ro și econsulat.ro
- Furt de date — Genpact România — Amendă 10.000 EUR
- Furt de date — Indaco Systems SRL
- Furt de date — SC Hayat Dent SRL — Amendă 2.000 EUR
- Furt de date — Your Consulting SRL — Amendă 3.000 EUR
- Furt de date — Tensa Art Design S.A — Amendă 20.000 EUR
- Furt de date — GENPACT ROMANIA SRL — Amendă 10.000 EUR
- Furt de date - Persoană fizică, al site-ului 0evita-teparii.ro - Amendă 10.000 EUR
- Furt de date — Money Seeds S.R.L.

LISTĂ SURSĂ ATACURI

- ING Bank — Amendată 4.000 EUR pentru divulgarea neautorizată a datelor client
- Furt de date — Comisia Europeană
- Renault România — Amendată cu 125.000 EUR, record GDPR în România
- Acces neautorizat — Emailul directorului FBI
- Acces neautorizat — Startupul Mercor
- Ransomware paralizează Apele Române — 1.000 sisteme blocate în 10 județe
- Grup rus NoName057 atacă MAI și Ministerul Justiției în ziua alegerilor
- Atac ransomware — Babuk la France Telecom Orange, Orange România
- Furt de date — SC Elite Conta SRL
- Atac cibernetic - Webrasoft Oradea CNP & IBAN expuse. Amendă: 20.000 EUR
- Furt de date — Accounting Audit SRL — Amendă 10.000 EUR
- Vodafone România amendată 4.000 EUR — date clienți accesate ilegal
- Atac cibernetic la firma de mobilă din Oradea — amendă 8.000 EUR
- Atac cibernetic — au fost vizate instituții-cheie ale statului,
- Ransomware "Gentlemen" blochează CEO — ERP și email inactive
- Atac cibernetic — firma CVA Tax & Finance SRL.
- Atac cibernetic — OnlyFans
- Atac cibernetic — medici de familie din Bihor
- Atac DDoS — Creditcoop
- Atac DDoS — Edificium SRL
- Atac DDoS — Fondul Garantare a Depozitelor Bancare
- Atac DDoS — Exim Bank
- Atac DDoS — Compania Națională de Administrare a Infrastr

LISTĂ SURSĂ ATACURI

- Atac DDoS — Mol România
- Furt de date — Incidentul de la Festivalul de Film de la Ven
- Atac DDoS asupra FCSB — site blocat în ziua vânzării biletelor cu Lyon
- NTT Data România — 230 GB date angajați furate. Amendă: 25.000 EUR
- Ransomware „Gentlemen” blochează CEO — ERP și email inactive
- Fraudă bancară — S.C. PRIMONET RO SRL — Amendă 20.000 EUR
- Atac DDoS asupra FCSB — site blocat în ziua vânzării biletelor cu Lyon
- Atac cibernetic — Firma de impresariat a lui Rareș Pop, victima
- Fraudă cibernetică — medici din Bihor rămași fără 1 milion lei
- Fraudă bancară — Vellea Home SRL — Amendă 5.000 EUR
- NTT Data România — 230 GB date angajați furate. Amendă: 25.000 EUR
- Furt de date — Agricola International SA — Amendă 5.000 EUR
- Atac ransomware — AAylex ONE, „grupul integrat din industria al
- Furt de date — DELIVERY SOLUTIONS S.A. — Amendă 2.000 EUR
- Atac cibernetic la Greencorp Oradea — date bancare angajați expuse. Amendă: 3.000 EUR
- Furt de date — AG-BROKER ASIGURARE S.R.L — Amendă 5.000 EUR
- Furt de date — Farmec S.A
- Furt de date — Poliției de Penitenciare
- Atac DDoS pe site-ul SRI — 19 milioane requesturi blocate de Cloudflare
- Atac DDoS — Bursa de Valori București
- Atac DDoS — Compania Națională Aeroporturi Bucuresti
- Atac DDoS — Astra Trans Carpatica Feroviar,
- Atac DDoS — Aeroportul Băneasa
- Atac DDoS — Ministerul Dezvoltării Lucrărilor Publice si
- Atac DDoS — Primăria Municipiului București
- Atac DDoS — Ministerul Turismului
- Furt de date — CECCAR
- Furt de date — NEW GAMBLING SOLUTIONS S.R.L. — Amendă 2.000 EUR
- Furt de date — IG Sports Management, Agentul FIFA Rareș Pop

LISTĂ SURSĂ ATACURI

- Furt de date — Google Calendar
- Furt de date — Dr. Max SRL — Amendă 1.000 EUR
- Furt de date — Continental Automotive Products SRL — Amendă 15.000 EUR
- Furt de date — Roumasport S.R.L — Amendă 10.000 EUR
- Acces neautorizat — PFA Nițu A. Cleopatra – Expert contabil — Amendă 2.000 EUR
- Furt de date — Cucina di Fabio S.R.L. — Amendă 2.000 EUR
- Furt de date — Whitedecor SRL — Amendă 2.000 EUR
- Furt de date — Agency for Control of Outstanding Debts S.R.L — Amendă 2.000 EUR
- Furt de date — S.P.E.E.H. HIDROELECTRICA SA
- Furt de date — PRIME TRANSACTION SA — Amendă 2.000 EUR
- Furt de date — CORAL TRAVEL & TOURISM SERVICES S.R.L.
- EON Energie amendată 25.000 EUR — parole clienți accesate neautorizat
- Furt de date — Unita Turism Holding S.A — Amendă 5.000 EUR
- Fraudă bancară — La Fântâna S.R.L. — Amendă 10.000 EUR
- Fraudă bancară — Asociația Casa de Ajutor Reciproc „FLEXICREDI — Amendă 3.000 EUR
- Furt de date — Georgescu Călin — Amendă 10.000 EUR
- Furt de date — SC Tremend Software Consulting SRL — Amendă 3.000 EUR
- Furt de date — Selgros Cash & Carry SRL — Amendă 3.000 EUR
- Atac cibernetic — SC Piramida Trade Invest SRL — Amendă 3.000 EUR
- Bitdefender amendată 10.000 EUR — date clienți divulgate prin eroare update
- Grupul Electrica lovit de ransomware — sute de servere blocate
- Ransomware Backmydata blochează 26 de spitale din România
- Hackerii cer 5 milioane dolari Primăriei Sector 5 București
- Atac ransomware — Companiile SoftTehnica și FreyaPOS
- Atac ransomware — Societatea Binbox Global Services
- Atac ransomware — Compania Dotro Telecom



LISTĂ SURSĂ ATACURI

- Hackerii sparg Camera Deputaților — datele lui Ciolacu pe dark web
- Hackerii fură transferul lui Coman — 6,25 milioane EUR redirectionate
- Atac ransomware — Institutul de Fonoaudiologie și Chirurgie Fun
- Atac ransomware — Spitalul de Pneumoftiziologie Roșiorii de Ved
- Atac ransomware — Clinica Sante Călărași
- Atac ransomware — Spitalul Orășenesc Băicoi
- Atac ransomware — Spitalul de Pediatrie Pitești
- Atac ransomware — Sanatoriul de Pneumoftiziologie Brad, Hunedoa
- Atac ransomware — Spitalul Județean de Urgență Buzău
- Atac ransomware — Spitalul Județean de Urgență "Dr. Constantin
- Atac ransomware — Spitalul Județean de Urgență Slobozia
- Atac ransomware — Spitalul Clinic Județean de Urgență "Sf. Apos
- Atac ransomware — Spitalul Județean de Urgență Pitești
- Atac ransomware — Spitalul Militar de Urgență "Dr. Alexandru Ga
- Atac ransomware — Institutul de Boli Cardiovasculare Timișoara
- Atac ransomware — Spitalul Municipal Sighetu Marmației
- Atac ransomware — Spitalul Județean de Urgență Târgoviște
- Atac ransomware — Spitalul Clinic Colțea
- Atac ransomware — Spitalul Municipal Medgidia
- Atac ransomware — institutul Clinic Fundeni
- Atac ransomware — Institutul Oncologic "Prof. Dr. Al. Trestiore
- Atac ransomware — Institutul Regional de Oncologie Iași
- Atac ransomware — Spitalul de Ortopedie și Traumatologie Azuga
- Atac ransomware — Spitalul orășenesc Băicoi
- Atac ransomware — Spitalul Clinic de Urgență Chirurgie Plastică
- Atac ransomware — Spitalul de Boli Cronice Sf. Luca
- Atac ransomware — Spitalul Clinic C.F. nr. 2 București
- Furt de date — Centrul medical MALP SRL Moinești
- Atac cibernetic — Mănăstirica Dragomirna
- Atac ransomware — Spitalul de Boli Cronice Smeeni



LISTĂ SURSĂ ATACURI

- Ransomware simultan: Primăria Timișoara, Poliția Locală și Direcția Fiscală
- Atac ransomware — Poliția Locală
- Atac ransomware — Direcția Fiscală
- Atac ransomware — Spitalul "Marius Nasta"
- Acces neautorizat — Lemken, specialistul în utilaje agricole
- Hackerii pro-ruși NoName75 atacă BCR, Alpha Bank și Banca Transilvania
- Altex România amendată 20.000 EUR — parole și carduri clienți publicate online
- Furt de date — Poliției Locale Suceava și cel al Spitalului
- Furt de date — Sanatoriul din Brad
- Furt de date — Spitalul Municipal din Caransebeș
- Furt de date — Site-ul DNSC a fost atacat de hackeri, cu o po
- Furt de date — rețelele de socializare, tik-tok
- Fraudă bancară — Compania-mamă a Lidl și Kaufland
- Furt de date — Facebook Marketplace
- Furt de date — Pagina de Facebook a Societății de Transport
- Acces neautorizat — Marcel Ciolacu, Kelemen Hunor.
- Atac ransomware — Softehnica S.R.L. — Amendă 5.000 EUR
- Atac ransomware la Primăria Bistrița — variantă nouă identificată de DNSC
- Atac ransomware — site-ul Inspectoratul Teritorial pentru Calit
- Hackerii sparg canalul YouTube al lui Selly — 3 milioane abonați afectați
- Furt de date — site-ul Primăriei Alba Iulia
- Acces neautorizat — Site-ul Ministerului Educației
- Fraudă bancară — ziarului BURSA
- Furt de date — Farmacia Ardealul SRL — Amendă 2.500 EUR
- Atac DDoS — site-ul băncii OTP Bank — Amendă 3.000 EUR
- Val DDoS Killnet — gov.ro, Armată, CFR, frontieră blocate simultan
- Atac DDoS — mapn.ro
- Atac DDoS — politiadefrontiera.ro
- Atac DDoS — cfrcalatori.ro
- Ransomware la Rompetrol — sistem Fill&Go și site-uri compromise. Amendă: 4.000 EUR



LISTĂ SURSĂ ATACURI

- Atac ransomware — Retailerul METRO
- Ransomware la Rompetrol — sistem Fill&Go și site-uri compromise. Amendă: 4.000 EUR
- Atac DDoS — Ministerului Apărării Naționale
- Acces neautorizat — Pagina de internet a aeroportului Otopeni
- Furt de date — utilizatorii serviciilor de telefonie să nu d
- Atac DDoS — Mai multe site-uri guvernamentale, printre ca
- Atac ransomware la Primăria Oradea — servicii cu publicul suspendate
- Atac cibernetic la Politehnica București — date studenți extrase
- Ransomware la primul spital din România — Spitalul Municipal Oradea, 2020
- Atac ransomware — AVON Firma internaționala
- Atac ransomware — sălile de jocuri de noroc(nu mentoinea num
- Atac ransomware — Atacul Maskirovka de 10 Miliarde de Dolari
- Atac ransomware — Softtehnica S.R.L — Amendă 5.000 EUR

217 atacuri.

459.000 EUR

în amenzi.

**Ești pregătit
sau ești următorul?**



DEFORCE TEHNOLOGIC

deforce.eu

<https://deforce.eu>