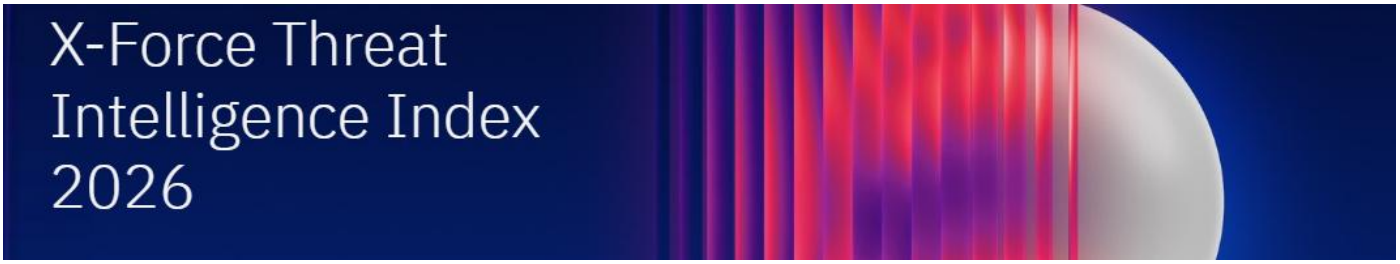


https://www.ibm.com/reports/threat-intelligence

Pregătește-te pentru atacuri accelerate de AI	Pe măsură ce atacatorii folosesc inteligența artificială pentru a scala operațiunile, liderii din domeniul securității trebuie să utilizeze inteligența artificială pentru a-și securiza proactiv oamenii, datele și infrastructura. Explorați Indexul de informații despre amenințările X-Force al IBM pentru a afla despre provocările cu care se confruntă echipele de securitate din întreaga lume și soluțiile adecvate de protecție.

44%	56%	300.000	49%
Creștere de la an la an a exploatării aplicațiilor software sau de sistem orientate spre public	Rata vulnerabilităților publicate care nu au necesitat autentificare pentru a fi exploatate	Numărul de credențiale de ChatGPT observate pentru vânzare pe dark web	Creștere a grupurilor ransomware active față de anul precedent

SUMAR

Cele mai importante tendințe observate de echipa IBM X-Force în 2025 au fost creșterea exploatărilor pe scară largă ale sistemelor expuse, puncte slabe ale lanțurilor de aprovizionare (supply-chain) cu software și dependențele sistemice tot mai mari în ecosistemele cloud și de aplicații.

Anul trecut, atacatorii și-au rafinat tehnicile de infiltrare a canalelor de distribuție a software-ului, a serviciilor cloud și a ecosistemelor open-source. Procedând astfel, au demonstrat cum un singur punct slab într-un mediu interconectat poate permite acces la scară largă sau cu privilegii de acces ridicate.

X-Force, care a extras date din testele de răspuns la incidente și de penetrare, din Dark-web și din alte surse de informații despre amenințări pentru acest raport, a identificat principalul vector inițial de acces: **exploatarea aplicațiilor orientate spre public**. Echipa a remarcat numărul tot mai mare și complexitatea vulnerabilităților software - combinate cu configurații greșite în aplicații - iar **adoptarea inteligenței artificiale a lărgit suprafața de atac pentru intruziuni**. Multe vulnerabilități nu au necesitat deloc autentificare, subliniind nevoia critică de controale de acces mai puternice, aplicare riguroasă de patch-uri și practici de implementare sigure.

X-Force a constatat, de asemenea, că furtul de acreditări a rămas în centrul multor campanii importante. Între timp, adoptarea rapidă a platformelor chatbot cu inteligență artificială pentru consumatori și utilizatorii de la locul de muncă a introdus un nou nivel de expunere; acreditările legate de acești chatbots au apărut din ce în ce mai mult pe piețele clandestine, determinate în mare parte de infecțiile cu infostealer pe dispozitivele utilizatorilor finali.

Tacticile dintre actorii statali persistenti (APTs) și grupurile infracționale cibernetice au continuat să convergă. X-Force a observat că instrumentele, tehnicile și modelele operaționale se suprapun din ce în ce mai mult între aceste comunități de amenințări, complicând atribuirea și întârziind potențial acțiunile de răspuns adecvate.

În mai multe cazuri, **activități care inițial păreau banale s-au dovedit ulterior a face parte din operațiuni persistente și extrem de sofisticate**.

Per total, anul 2025 a evidențiat un mesaj clar: protecția identității, configurația securizată și vizibilitatea în aplicații, procese de dezvoltare și medii cloud sunt din ce în ce mai importante pentru reziliența cibernetică.

Inteligența artificială a continuat, de asemenea, să remodeleze operațiunile atacatorilor în 2025. Deși IA nu a schimbat strategiile, aceasta a crescut dramatic viteza, amploarea și eficiența acestor operațiuni. Adversarii folosesc acum IA generativă pentru a reduce ciclurile de decizie, a scala ingineria socială și a itera pe căile de atac în timp real. Pe măsură ce modelele multimodale se maturizează, bariera la intrare se va micșora și mai mult, permițând lucrătorilor cu calificare mai scăzută să automatizeze recunoașterea, escaladarea privilegiilor și mișcarea laterală, rezultând o mișcare mai rapidă și amenințări mai adaptive.

În ciuda acestor tendințe în evoluție și uneori a amenințărilor sofisticate, lacunele de bază în igiena securității cibernetice au contribuit la multe compromisuri; misiunile de răspuns la incidente și de testare a penetrării X-Force au constatat controale de acces greșit configurate, practici de autentificare slabe, înregistrare incompletă și gestionare insuficientă a vulnerabilităților ca probleme recurente. Aceste slăbiciuni fundamentale au continuat să ofere atacatorilor oportunități mult mai ușor de exploatat decât tehnicile avansate sau noi.

Aspecte principale ale raportului

- Creștere de 44% în exploatarea aplicațiilor către public

X-Force a observat o creștere a exploatării aplicațiilor accesibile publicului ca vector de acces inițial în 2025, din cauza unei creșteri a atacurilor asupra lanțului de aprovizionare (supply-chain) care vizează ecosistemele de dezvoltare și infrastructura de încredere.

- 56% din vulnerabilitățile dezvăluite nu necesitau autentificare pentru a fi exploatate cu succes

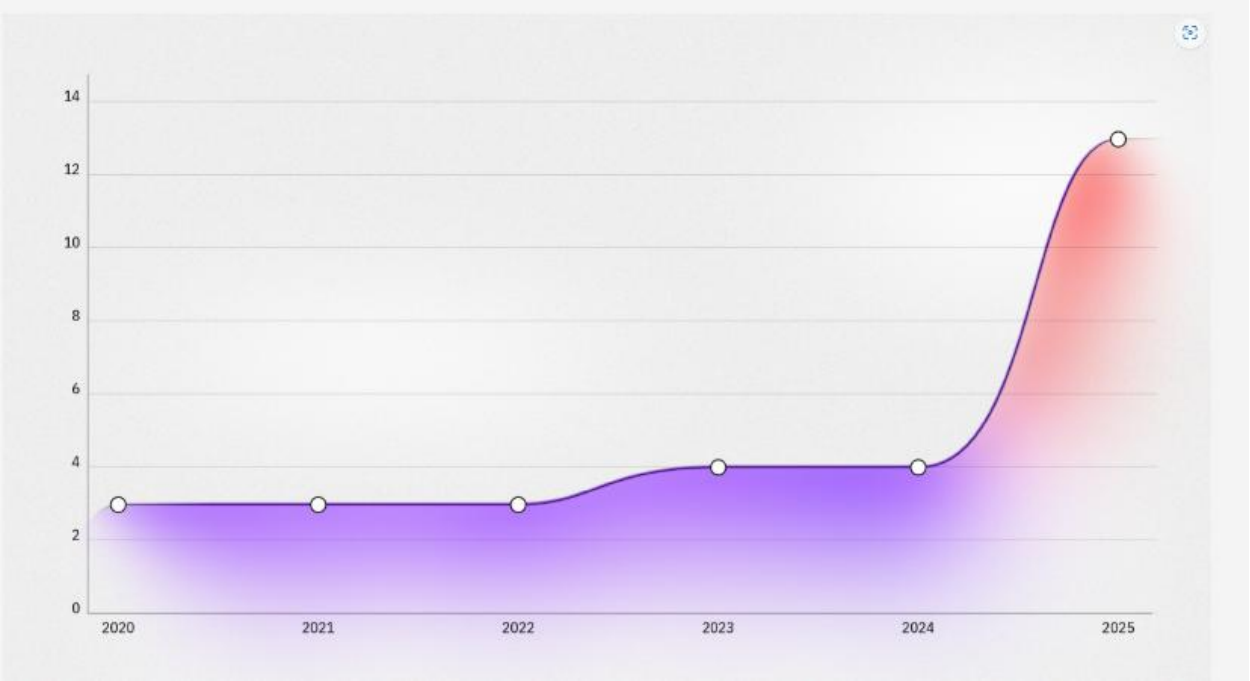
Numărul vulnerabilităților urmărite de X-Force a ajuns aproape de 40.000 în 2025, iar mai bine de jumătate nu necesitau autentificare pentru ca un atacator să le exploateze cu succes. Această constatare ar putea reflecta lacune în implementarea securității din design, deoarece atacatorii reușesc fără a folosi credentiale, ocolirea MFA sau chiar interacțiunea cu utilizatorul final.

- >300.000 de conturi ChatGPT observate de vânzare pe dark web

În 2025, **malware-ul de tip infostealer a dus la expunerea a peste 300.000 de conturi ChatGPT**, demonstrând că platformele AI au ajuns să aibă același risc pentru conturi ca și alte soluții SaaS esențiale pentru companii. Deși niciunul dintre conturile postate nu mai era valabil, acestea corespundeau constant cu infecții cauzate de infostealer și cu colecții de conturi scurse observate în 2024 și anterior.

- X-Force a urmărit aproape 40.000 de vulnerabilități în 2025. **Peste jumătate nu necesitau autentificare pentru ca un atacator să le exploateze cu succes.**
- Adversarii au exploatat tot mai mult încrederea dezvoltatorilor și integrarea identităților pentru a fura acreditările, a pătrunde în mediile cloud și a menține persistența în sistemele interconectate. Dependențele extinse de terți creează suprafețe de atac greu de securizat – unde un singur punct slab poate expune multe ținte. Odată, aceste tehnici de atac asupra lanțului de aprovizionare erau în mare parte folosite de actori statali, dar acum sunt adoptate și de grupuri criminale motivate financiar și alte grupuri infracționale, reflectând o clară răspândire a tacticilor avansate.
- **Creștere de 49% a grupurilor active de ransomware** comparativ cu 2024
- Fragmentarea continuă în acest spațiu, cu 109 grupuri diferite de extorcare ransomware identificate de X-Force în 2025. Față de 73 de grupuri în 2024, această fragmentare reflectă o barieră de intrare mai mică: actorii rău intenționați folosesc frecvent unelte scurse, urmează planuri de atac deja stabilite sau trec între identități de grup, permițând multor operatori mici să desfășoare atacuri oportuniste, cu volum redus.

- Cele mai vizate sectoare: Industria de producție (27,7% din incidente, față de 26% anul precedent; Si sectoarele de finanțe și asigurări, care au reprezentat 27% în 2025 și 23% în 2024.
- 29% dintre atacuri au vizat America de Nord; Regiunea a reprezentat aproape o treime din totalul cazurilor. În creștere față de 24% în 2024, America de Nord a devenit regiunea cea mai atacată pentru prima dată în 6 ani. În schimb, Asia Pacific a văzut o scădere de la 34% la 27%.
- În ultimii 5 ani, s-a înregistrat o **creștere de aproape 4 ori a numărului de compromiteri majore ale lanțului de aprovizionare sau ale terților**. Adesea, o singură încălcare a securității la un furnizor de încredere s-a răspândit la mulți clienți din aval, ducând la infiltrare pe scară largă, perturbări sau furt de date.



Grafic: Cresterea breșelor din „supply chain /third-party" - Sursa: IBM X-Force report 2026

Inteligența artificială (AI) în securitatea cibernetică ofensivă

Inteligența artificială nu mai este un concept emergent în securitatea cibernetică. Este un multiplicator de forță folosit activ atât de apărători, cât și de adversari. Actorii rău intenționați aplică deja AI generativ pentru a scala operațiunile de phishing, a accelera dezvoltarea codului malițios și a îmbunătăți ingineria socială prin calitatea și realismul limbajului. În același timp, apărătorii folosesc analiză bazată pe AI pentru a procesa volume uriașe de telemetrie, a identifica comportamente anormale și a scurta timpii de detectare și răspuns.

Totuși, este important să recunoaștem că **AI nu a schimbat fundamentele campaniilor de atac cibernetic. Atacatorii se bazează în continuare pe vulnerabilități neactualizate, acreditări valide și configurări greșite pentru a-și îndeplini obiectivele. Ceea ce AI a schimbat este viteza, amploarea și eficiența acestor atacuri, ceea ce face ca detectarea rapidă și răspunsul decisiv să fie mai importante ca niciodată**.

Ceea ce începe cu imitarea asistată de AI și manipularea limbajului adesea escaladează în ceva mult mai semnificativ. Sistemele multimodale au capacitatea de a extinde aceste avantaje dincolo de ingineria socială, în fluxuri de lucru de intruziune tehnică. Pe măsură ce modelele AI multimodale se maturizează, adversarii vor putea automatiza sarcini tot mai complexe — inclusiv recunoașterea, escaladarea privilegiilor și mișcarea laterală — creând amenințări mai rapide și mai adaptative.

Transformarea cea mai substanțială în curs nu este crearea unor metode noi de atac, ci democratizarea capacităților avansate, unde **grupuri mai puțin experimentate sau slab dotate pot acum să execute operațiuni care anterior necesitau expertiză aprofundată.**

AI oferă, de asemenea, avantaje atacatorilor prin adoptarea asimetrică. Adversarii se confruntă cu mai puține constrângeri legate de guvernanță, siguranță și responsabilitate, ceea ce le permite să adopte și să pună în aplicare noi capabilități mai rapid decât majoritatea companiilor. Ca urmare, utilizarea defensivă a inteligenței artificiale nu oferă automat un avantaj. Fără date de înaltă calitate, procese mature și o integrare clară în operațiunile de securitate, apărările bazate pe AI pot întâmpina dificultăți în a ține pasul cu adversarii care pot testa, elimina și perfecționa rapid tehnici fără supraveghere.

Recomandari si actiuni utile:

- Pregătiți-vă pentru atacuri accelerate de IA - unde viteza, scalarea și automatizarea sparg apărarea tradițională

• Monitorizați identitățile umane și non-umane - și detectați amenințările - cu IA

• Integrați controale de identitate în securitatea aplicațiilor și API-urilor

• Testați și căutați vulnerabilități: Cod nesigur, Acreditări slabe sau reutilizate, Configurații greșite, Modificări neautorizate, Setări implicite nesigure, Comportament riscant al utilizatorilor, Lipsa patch-urilor

• Prioritizați securitatea platformei IA.

o Liderii în domeniul securității au nevoie de o soluție cuprinzătoare de **guvernanță AI** pentru a scala AI cu încredere și transparență și într-un mod care generează valoare. Pentru a evita dependenta de furnizor, soluția ar trebui să fie deschisă, hibridă și agnostică față de platformă, ceea ce înseamnă că organizațiile pot utiliza modelul potrivit pentru cazul de utilizare potrivit și își pot implementa IA acolo unde are cel mai mult sens.

o Guvernanța modelului permite evaluarea IA subiacentă, pentru a testa performanța, acuratețea și a proteja împotriva comportamentului neadecvat.

o Organizațiile ar trebui să evalueze adoptarea IA în întreaga întreprindere, inclusiv aplicarea unei autentificări puternice și a controalelor de acces condiționat, securizarea sistemelor IA, protejarea acreditărilor și token-urilor serviciilor IA și monitorizarea modelelor de acces anormale sau a expunerii acreditărilor.

• Cartografiați-vă amprenta și urmăriți semnalele observate de atacatori

• Accelerați securitatea datelor. Controale corecte de protecție a datelor - cum ar fi criptarea, controalele de acces, prevenirea pierderii de date, monitorizarea și auditarea și clasificarea securizată a datelor - pentru a securiza datele organizaționale și a gestiona datele care sunt introduse în inteligența artificială pentru a preveni expunerea accidentală a datelor sensibile.

Atacurile cibernetice evoluează mai rapid ca niciodată. X Force Threat Intelligence Index din acest an dezvăluie modul în care atacatorii folosesc inteligența artificială pentru a exploata lacunele fundamentale de securitate pentru a obține acces inițial și a compromite scalarea.

NEXT:

- Programați o sesiune informativă X-Force Threat Intelligence Index 2026 („discovery briefing”) de o oră. Include o interacțiune individuală cu un analist X-Force care vă poate ajuta să înțelegeți cum poate îmbunătăți postura de securitate cibernetică a organizației
  Threat Intelligence Index Form 2026 https://www.ibm.com/forms/mkt-15072
- Obțineți raportul : X-Force Threat Intelligence Index 2026 | IBM https://www.ibm.com/reports/threat-intelligence
- înregistrați-vă/urmăriți webinarul. The 2026 X-Force Threat Intelligence Index: Critical Insights on AI, Vulnerabilities and Supply-Chain Risk - 1752695