# INTELLIGENCE INFO

ISSN 2821 - 8159, ISSN – L 2821 – 8159, Volumul 3, Numărul 1, Martie 2024

# Atacurile cibernetice avansate care vizează guvernele: provocări și soluții

Nicolae Sfetcu

Sfetcu, Nicolae (2024), Integrarea inteligenței artificiale în serviciile de informații, *Intelligence Info*, **3**:1, 3-10, DOI: 10.58679/II77703, https://www.intelligenceinfo.org/atacurile-cibernetice-avansate-care-vizeaza-guvernele-provocari-si-solutii/

Publicat online: 09.02.2024

# Atacurile cibernetice avansate care vizează guvernele: provocări și soluții

Ing. fiz. Nicolae SFETCU, MPhil[1]
nicolae@sfetcu.com

## Advanced Cyber Attacks Targeting Governments: Challenges and Solutions

**Abstract**

In today's digital landscape, governments face unprecedented challenges in securing their cyber infrastructure against advanced attacks. The proliferation of sophisticated cyber threats poses significant risks to national security, economic stability, and public trust. Advanced cyber attack tactics continue to evolve, requiring continuous adaptation of cyber security strategies. Integrating artificial intelligence and machine learning into cyber security solutions is becoming increasingly vital in the fight against advanced cyber attacks.

This essay examines the nature of advanced cyber attacks targeting governments, the factors that contribute to their proliferation, and proposes solutions to mitigate these threats.

**Keywords**: cyber attacks, advanced persistent threats, ransomware, artificial intelligence, Internet of Things, spear phishing, social engineering, cyber espionage

**Rezumat**

În peisajul digital contemporan, guvernele se confruntă cu provocări fără precedent în securizarea infrastructurii lor cibernetice împotriva atacurilor avansate. Proliferarea amenințărilor cibernetice sofisticate prezintă riscuri semnificative pentru securitatea națională, stabilitatea economică și încrederea publicului. Tacticile atacurilor cibernetice avansate continuă să evolueze, necesitând o adaptare continuă a strategiilor de securitate cibernetică. Integrarea inteligenței artificiale și a învățării automate în soluțiile de securitate cibernetică devine din ce în ce mai vitală în lupta împotriva atacurilor cibernetice avansate.

Acest eseu examinează natura atacurilor cibernetice avansate care vizează guvernele, factorii care contribuie la proliferarea acestora și propune soluții pentru a atenua aceste amenințări.

**Cuvinte cheie**: atacuri cibernetice, amenințări persistente avansate, ransomware, inteligența artificială, Internetul obiectelor, spear phishing, inginerie socială, spionaj cibernetic

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

INTELLIGENCE INFO, Volumul 3, Numărul 1, Martie 2024, pp. 3-10
ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II77703
URL: https://www.intelligenceinfo.org/atacurile-cibernetice-avansate-care-vizeaza-guvernele-provocari-si-solutii/


## Introducere

În peisajul digital contemporan, guvernele se confruntă cu provocări fără precedent în securizarea infrastructurii lor cibernetice împotriva atacurilor avansate. Proliferarea amenințărilor cibernetice sofisticate prezintă riscuri semnificative pentru securitatea națională, stabilitatea economică și încrederea publicului. Acest eseu examinează natura atacurilor cibernetice avansate care vizează guvernele, factorii care contribuie la proliferarea acestora și propune soluții pentru a atenua aceste amenințări.

Atacurile cibernetice avansate care vizează guvernele cuprind un spectru larg de tactici, tehnici și proceduri folosite de actori de amenințări sofisticați. Aceste atacuri folosesc adesea tehnologii de ultimă oră, cum ar fi inteligența artificială, învățarea automată și automatizarea pentru a ocoli măsurile tradiționale de securitate. De la spionaj sponsorizat de stat la campanii de ransomware, aceste atacuri prezintă riscuri multiple pentru guvernele din întreaga lume.

Tacticile atacurilor cibernetice avansate continuă să evolueze, necesitând o adaptare continuă a strategiilor de securitate cibernetică. Integrarea inteligenței artificiale și a învățării automate în soluțiile de securitate cibernetică devine din ce în ce mai vitală în lupta împotriva atacurilor cibernetice avansate.

## Tipuri de atacuri cibernetice

Spionajul cibernetic sponsorizat de stat rămâne o amenințare predominantă, statele naționale căutând să fure informații sensibile, să perturbe infrastructura critică sau să submineze procesele politice. Amenințările persistente avansate (APT) orchestrate de statele-națiune implică adesea operațiuni sub acoperire pe termen lung care vizează

infiltrarea în rețele guvernamentale, exfiltrarea datelor clasificate și desfășurarea activităților de colectare de informații. Exemple notabile includ presupusa intervenție a Rusiei în alegerile prezidențiale din SUA din 2016 și campania de spionaj cibernetic din China, cunoscută sub numele de APT10, care vizează entități și corporații guvernamentale.

În plus, creșterea atacurilor ransomware pune provocări semnificative pentru agențiile guvernamentale la toate nivelurile. Operatorii de ransomware folosesc tehnici de criptare sofisticate pentru a cripta datele critice, solicitând plăți de răscumpărare în schimbul cheilor de decriptare. Aceste atacuri nu numai că perturbă operațiunile guvernamentale, ci și impun sarcini financiare substanțiale și subminează încrederea publicului. Atacul ransomware Colonial Pipeline din 2021 din Statele Unite a evidențiat impactul devastator al unor astfel de atacuri asupra infrastructurii critice și a securității naționale.

Atacurile persistente avansate (APT) sunt amenințări sofisticate, specifice și în evoluție, dar anumite modele pot fi identificate în procesul lor. Contramăsurile tradiționale nu sunt suficiente pentru protecția împotriva APT. Potențialele victime trebuie să obțină o înțelegere de bază a etapelor și tehnicilor implicate în atacuri, pe baza cărora să dezvolte capabilități specifice.

**Caracteristicile amenințărilor persistente avansate**

APT-urile se caracterizează prin natura lor ascunsă, prelungită și direcționată. Actorii din spatele APT folosesc tehnici avansate, cum ar fi exploit-uri zero-day, inginerie socială și malware polimorf ca să rămână nedetectate pentru perioade îndelungate. Înțelegerea acestor caracteristici este crucială pentru dezvoltarea eficientă de mecanisme de detectare.

Există anumite simptome ale atacurilor APT, inclusiv[2]:

1. Activitate neobișnuită în conturile de utilizator
2. Detectarea programelor malware de tip troian backdoor pentru acces, prin o activitate neobișnuită a bazei de date
3. Prezența unor fișiere de date neobișnuite
4. Anomalii în datele de ieșire.

[2] (Yasar și Rosencrance 2021)

## Evoluția tacticilor APT

Pe măsură ce tehnologia avansează, la fel evoluează și tacticile folosite de APT. Aceasta secțiune explorează strategiile în evoluție ale APT-urilor, inclusiv utilizarea inteligenței artificiale, învățare automată și canale de comunicare criptate pentru evitarea măsurilor tradiționale de detectare. Examinarea acestor tactici este vitală pentru a rămâne în jocul în curs de desfășurare între apărători și actorii amenințării.

Conform lui Zou et al.[3], abordările curente ale detectării APT de jos în sus (de ex., urmărirea provenienței - a fluxului de informații) încearcă să deducă existența tacticii APT din informații de nivel scăzut. Recunoașterea APT5,6,7,8 se bazează în principal pe „conectarea punctelor" nesupravegheate prin urmărirea provenienței. Aceste abordări efectuează mai întâi analiza dependenței de activitate și construcția graficului de cauzalitate, apoi folosesc euristici pentru a simplifica graficele rezultate, analizându-le. Unul din dezavantajele acestei abordări este problema exploziei dependenței, bine cunoscută în criminalistica digitală.

Abordările de sus în jos profită de cunoștințele despre APT cunoscute ocolind problema exploziei dependenței. Ele se bazează pe modele de funcționare a unor APT, precum Stuxnet, nefiind necesară învățarea nesupravegheată a asociațiilor. De exemplu, HOLMES folosește ciclul de viață APT ca model de atac și apoi încearcă să se potrivească cu fiecare pas[4] HOLMES adună date de audit de computer și clasifică gravitatea atacurilor APT în timp real, luând în considerare șapte etape ale așa-numitului „lanț de distrugere".

## Vulnerabilități

Mai mulți factori contribuie la proliferarea atacurilor cibernetice avansate care vizează guvernele. În primul rând, interconectarea tot mai mare a sistemelor digitale și dependența de tehnologiile emergente creează noi suprafețe de atac și vulnerabilități. Adoptarea rapidă a cloud computingului, a dispozitivelor Internet of Things (IoT) și a infrastructurii de lucru la distanță extinde vectorul de atac pe care adversarii îl pot exploa. În plus, economia subterană a criminalității cibernetice a devenit din ce în ce mai

[3] (Zou et al. 2020)
[4] (Milajerdi et al. 2019)

sofisticată, permițând actorilor amenințărilor să achiziționeze instrumente și servicii avansate pe dark web.

Mai mult, tensiunile geopolitice și lipsa normelor internaționale care guvernează spațiul cibernetic exacerba peisajul amenințărilor. Statele-națiune se angajează în operațiuni cibernetice în scopuri strategice, inclusiv spionaj, sabotaj și constrângere, ceea ce duce la o stare perpetuă de conflict cibernetic. Atribuirea atacurilor cibernetice rămâne o provocare, permițând făptuitorilor să opereze cu impunitate și să se sustragă la răspundere. Absența unor reguli de implicare universal acceptate în spațiul cibernetic complică și mai mult eforturile de descurajare a actorilor rău intenționați și de a preveni escaladarea.

## Oportunități și provocări

Natura atacurilor cibernetice avansate este în sine o provocare, datorită caracteristicilor specifice ale acestor atacuri: atacatori hotărâți și puternici, durata lungă a atacurilor, vulnerabilitățile angajaților interni exploatate prin inginerie socială, și infrastructura rețelelor când mediul folosește resurse de cloud computing.

Atacurilor cibernetice avansate au mai multe caracteristici specifice care o fac mai dificil de detectat[5]:

- date dezechilibrate: semnale slabe printre cantități uriașe de date; spre deosebire de rețelele bot[6], în APT doar câteva gazde sunt infectate;
- problema ratei de bază: evenimente foarte rare care se întind pe perioade lungi de timp[7];
- lipsa de date disponibile public: majoritatea companiilor victime nu au niciun interes să publice detalii ale unor astfel de evenimente;
- folosirea criptării și a protocoalelor standard: previne eficacitatea soluțiilor de securitate a rețelei[8].

## Soluții împotriva atacurilor cibernetice avansate

Pentru a aborda provocările generate de atacurile cibernetice avansate care vizează guvernele, este necesară o abordare cu mai multe fațete. În primul rând, guvernele trebuie

[5] (Marchetti et al. 2016)
[6] (Feily, Shahrestani, și Ramadass 2009)
[7] (Axelsson 2000)
[8] (Denning 1987)

să investească în capabilități solide de securitate cibernetică, inclusiv informații despre amenințări, sisteme de detectare a intruziunilor și capabilități de răspuns la incidente. Măsurile proactive de securitate cibernetică, cum ar fi evaluările regulate ale vulnerabilităților, testele de penetrare și instruirea angajaților sunt esențiale pentru a întări apărarea împotriva amenințărilor în evoluție.

Țările și organizațiile ar trebui să colaboreze pentru a partaja informații despre amenințări, ajutând la identificarea și răspunsul la campaniile atacurilor cibernetice mai eficient. Cooperarea și colaborarea internațională sunt cruciale pentru a atenua natura transnațională a amenințărilor cibernetice. Guvernele trebuie să lucreze împreună pentru a stabili norme de comportament responsabil al statului în spațiul cibernetic, pentru a promova schimbul de informații și asistența reciprocă și pentru a consolida eforturile diplomatice pentru a aborda amenințările cibernetice la nivel global. Inițiative precum Convenția de la Budapesta privind criminalitatea cibernetică și Apelul de la Paris pentru încredere și securitate în spațiul cibernetic servesc drept cadre pentru cooperarea internațională în combaterea criminalității cibernetice și consolidarea securității cibernetice. Dezvoltarea cadrelor juridice internaționale pentru abordarea APT poate permite monitorizarea și urmărirea penală a actorilor amenințărilor.

În plus, parteneriatele public-privat joacă un rol vital în creșterea rezistenței securității cibernetice. Colaborarea dintre agențiile guvernamentale, organizațiile din sectorul privat, mediul academic și societatea civilă poate facilita schimbul de bune practici, expertiză și resurse pentru a atenua eficient amenințările cibernetice. Platformele de partajare a informațiilor, cum ar fi Centrele de Partajare și Analiză a Informațiilor (ISAC), permit părților interesate să colaboreze în timp real și să coordoneze răspunsurile la incidentele cibernetice.

În atenuarea atacurilor cibernetice avansate, teoria jocurilor poate ocupa un loc important ca un model al competiției dintre un apărător și un atacator[9]. Elementele de incertitudine pot fi abordate cu noțiuni precum jocurile stocastice sau jocurile cu informații incomplete, sau folosind un model de jocuri matrice mai simplu și mai ușor de configurat, care ia în considerare faptul că timpul este discret pentru atacator dar continuu pentru

[9] (Rass, König, și Schauer 2017)

apărător. Perspectiva teoretică a jocului permite dezvoltarea unei strategii optime de apărare pornind aproape direct de la informațiile disponibile, evitând modelarea adversară.

În protecția împotriva atacurilor cibernetice avansate se pot utiliza tehnologii precum deep learning (SignalSense), o nouă abordare a securității rețelei, monitorizare constantă, adaptare și învățare prin experiență[10]. PwC, în Sondajul privind starea globală a securității informațiilor din 2015, observă că în cadrul organizațiilor, actualii (31%) sau foștii (27%) angajații sunt sursa principală a amenințărilor interne[11]. Ar trebui, de asemenea, să se acorde mai multă atenție monitorizării traficului pe baza rețelelor neuronale (detectori scalabili, clasificarea gazdei, IP, pachete și reputația de trafic) care caută anomalii față de modelul obișnuit. În general, strategiile de protecție includ, conform lui[12], schimbul integrat de informații între punctele de securitate, prevenirea și detectarea avansată, inclusiv o abordare strategică amplă (configurare hardware tactică și scenarii de atac), monitorizarea traficului SSL și asigurarea protecției depline.

Atacurile cibernetice avansate pot fi considerate una dintre cele mai preocupante probleme de securitate, în care IoT (Internetul obiectelor) ocupă un loc principal. În ciuda evoluției APT, unele abordări sau modele tradiționale pot fi încă utilizate pentru a detecta sau identifica astfel de atacuri. Pe baza comportamentului rețelei, se poate monitoriza rețeaua pentru activități suspecte și se poate acționa proactiv.

Cea mai obișnuită modalitate de a obține accesul inițial în rețele este prin inginerie socială, prin mesaje email de tip spear phishing către angajați. Prin urmare, organizațiile trebuie să își îmbunătățească programele de conștientizare a utilizatorilor; aspectul uman al atacurilor cibernetice avansate este foarte complex și trebuie abordat din perspectivă comportamentală, precum și din teoriile comportamentului de acțiune motivată.

Tehnicile și modelele de învățare automată utilizate frecvent pentru a detecta un atac cibernetic avansat sunt SVM, k-NN și DT, cu rezultate bune. Se recomandă crearea unui set de date care să conțină fluxuri de rețea (normale și rău intenționate) pentru a antrena algoritmii ML utilizați în cadru, iar eficiența cadrului poate fi testată prin simularea unui atac cibernetic avansat într-un spațiu controlat[13].

[10] (SignalSense 2015)
[11] (PWC 2014)
[12] (Rot și Olszewski 2017)
[13] (Quintero-Bonilla și Martín del Rey 2020)

## Concluzie

În concluzie, atacurile cibernetice avansate care vizează guvernele reprezintă provocări semnificative pentru securitatea națională, stabilitatea economică și încrederea publicului. Aceste atacuri exploatează vulnerabilități în infrastructura digitală, utilizează tehnologii avansate și sunt adesea orchestrate de actori sofisticați ai amenințărilor, inclusiv state naționale și organizații criminale cibernetice. Abordarea acestor provocări necesită o abordare cuprinzătoare care să cuprindă inovarea tehnologică, cooperarea internațională și parteneriatele public-privat. Investind în capacitățile de securitate cibernetică, promovând norme internaționale și încurajând colaborarea, guvernele își pot spori rezistența împotriva amenințărilor cibernetice avansate și pot proteja activele și infrastructura critice în era digitală.

## Bibliografie

Axelsson, Stefan. 2000. „The base-rate fallacy and the difficulty of intrusion detection". *ACM Transactions on Information and System Security* 3 (3): 186–205. https://doi.org/10.1145/357830.357849.

Denning, D.E. 1987. „An Intrusion-Detection Model". *IEEE Transactions on Software Engineering* SE-13 (2): 222–32. https://doi.org/10.1109/TSE.1987.232894.

Feily, Maryam, Alireza Shahrestani, și Sureswaran Ramadass. 2009. „A Survey of Botnet and Botnet Detection". *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, 268–73. https://doi.org/10.1109/SECURWARE.2009.48.

Marchetti, Mirco, Fabio Pierazzi, Michele Colajanni, și Alessandro Guido. 2016. „Analysis of high volumes of network traffic for Advanced Persistent Threat detection". *Computer Networks* 109 (iunie). https://doi.org/10.1016/j.comnet.2016.05.018.

Milajerdi, Sadegh M., Rigel Gjomemo, Birhanu Eshete, R. Sekar, și V.N. Venkatakrishnan. 2019. „HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows". În *2019 IEEE Symposium on Security and Privacy (SP)*, 1137–52. https://doi.org/10.1109/SP.2019.00026.

PWC. 2014. „Managing cyber risks in an interconnected world". https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Quintero-Bonilla, Santiago, și Angel Martín del Rey. 2020. „A New Proposal on the Advanced Persistent Threat: A Survey". *Applied Sciences* 10 (11): 3874. https://doi.org/10.3390/app10113874.

Rass, Stefan, Sandra König, și Stefan Schauer. 2017. „Defending Against Advanced Persistent Threats Using Game-Theory". *PLOS ONE* 12 (1): e0168675. https://doi.org/10.1371/journal.pone.0168675.

Rot, Artur, și Bogusław Olszewski. 2017. *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*. https://doi.org/10.15439/2017F488.

SignalSense. 2015. „Using Deep Learning To Detect Threat, SignalSense, White Paper”,. https://www.ten-inc.com/presentations/deep_learning.pdf.

Yasar, Kinza, și Linda Rosencrance. 2021. „What Is an Advanced Persistent Threat (APT)? | Definition from TechTarget”. Security. 2021. https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT.

Zou, Qingtian, Xiaoyan Sun, Peng Liu, și Anoop Singhal. 2020. „An Approach for Detection of Advanced Persistent Threat Attacks”, nr. 12 (decembrie): 92–26. https://doi.org/10.1109/MC.2020.3021548.