EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RAPORTUL ENISA PRIVIND SITUAȚIA AMENINȚĂRILOR 2021

Din aprilie 2020 până la jumătatea lunii iulie 2021

OCTOMBRIE 2021

DESPRE ENISA

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică contribuie la politica cibernetică a UE, îmbunătățește fiabilitatea produselor, a serviciilor și a proceselor TIC prin sistemele de certificare a securității cibernetice, cooperează cu statele membre și cu organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu principalele părți interesate pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, ca scop final, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa pot fi găsite aici: www.enisa.europa.eu.

CONTACT

Pentru a lua legătura cu autorii, vă rugăm să utilizați adresa etl@enisa.europa.eu.
Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.

EDITORI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agenția Uniunii Europene pentru Securitate Cibernetică

CONTRIBUITORI

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

MULȚUMIRI

Dorim să mulțumim membrilor și observatorilor Grupului de lucru ad-hoc al ENISA privind situația amenințărilor cibernetice, pentru feedbackul și comentariile valoroase pe care le-au oferit în vederea validării acestui raport. De asemenea, am dori să mulțumim Grupului consultativ al ENISA și rețelei ofițerilor naționali de legătură, pentru feedbackul lor valoros.
Am dori să mulțumim totodată echipelor ENISA care se ocupă de conștientizarea situației și de notificarea incidentelor, pentru contribuția lor activă și sprijinul acordat în coroborarea diferitelor informații pentru elaborarea raportului privind situația amenințărilor.

AVIZ JURIDIC

AVIZ PRIVIND DREPTURILE DE AUTOR

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

CUPRINS

REZUMAT

Aceasta este cea de-a noua ediție a raportului ENISA privind situația amenințărilor (ETL), un raport anual privind situația amenințărilor la adresa securității cibernetice, care identifică principalele amenințări, principalele tendințe observate în ceea ce privește amenințările, actorii care generează amenințări și tehnicile de atac și descrie, de asemenea, măsurile de atenuare relevante. În procesul de îmbunătățire continuă a metodologiei noastre de elaborare a raportului privind situația amenințărilor, activitatea din acest an a fost sprijinită de un grup de lucru ad-hoc nou format din cadrul ENISA pentru situația amenințărilor la adresa securității cibernetice.

Intervalul de timp vizat de raportul ETL 2021 este cuprins între aprilie 2020 și iulie 2021 și este denumit „perioada de raportare" în întregul raport. Pe parcursul perioadei de raportare, principalele amenințări identificate includ:

- **Ransomware (programe de șantaj digital)**
- **Malware**
- **Criptojacking**
- **Amenințări legate de e-mail**
- **Amenințări la adresa datelor**
- **Amenințări la adresa disponibilității și integrității**
- **Dezinformare - informare greșită**
- **Amenințări fără intenții răuvoitoare**
- **Atacuri în lanțul de aprovizionare**

În acest raport discutăm despre primele 8 categorii de amenințări la adresa securității cibernetice. Amenințările care vizează lanțurile de aprovizionare, a noua categorie, au fost analizate amănunțit, dată fiind importanța lor deosebită, într-un raport specific al ENISA intitulat „Raportul ENISA privind situația amenințărilor cu referire la atacurile care vizează lanțurile de aprovizionare"[1].

Pentru fiecare dintre amenințările identificate sunt luate în discuție tehnici de atac, incidente notabile și tendințe, împreună cu măsurile de atenuare propuse. În ceea ce privește tendințele, în timpul perioadei de raportare evidențiem următoarele aspecte:

- **Ransomware** a fost evaluat ca fiind **principala amenințare pentru perioada 2020-2021**.
- **Organizațiile guvernamentale și-au intensificat activitatea în acest sens** atât la nivel național, cât și internațional.
- **Infractorii cibernetici sunt din ce în ce mai motivați de monetizarea** activităților lor, de exemplu, ransomware. **Criptomonedele** rămân cea mai frecventă metodă de plată pentru actorii care generează amenințări.
- **Scăderea numărului de programe malware** care a fost observată în 2020 continuă și în cursul anului 2021. În 2021, am observat o creștere a numărului de actori care generează amenințări și care recurg la limbaje de programare relativ noi sau neobișnuite pentru a-și porta codul.
- Volumul **infectărilor de tip cryptojacking** a atins un **nivel record** în primul trimestru al anului 2021, comparativ cu ultimii ani. **Câștigul financiar** asociat activității de cryptojacking i-a stimulat pe actorii care generează amenințări să efectueze aceste atacuri.
- **COVID-19 este în continuare momeala dominantă în campaniile** de atacuri prin e-mail.
- S-a înregistrat o **creștere a numărului de încălcări ale securității datelor în sectorul sănătății**.
- În 2021, **campaniile DDoS (Distributed Denial of Service) tradiționale** sunt mai bine țintite, mai persistente și din ce în ce mai multivectoriale. **IoT (internetul lucrurilor)**, în combinație cu **rețelele mobile**, are ca rezultat un nou val de atacuri DDoS.

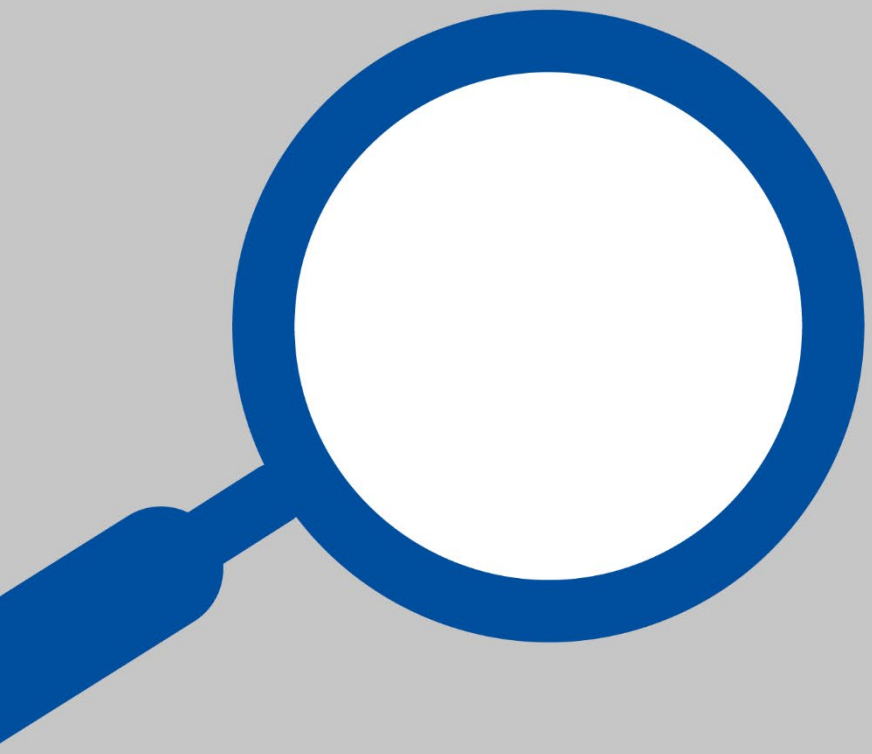
[1] ENISA Threat Landscape for Supply Chain Attacks (Raportul ENISA privind situația amenințărilor cu referire la atacurile care vizează lanțurile de aprovizionare), iulie 2021 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- În 2020 și 2021, observăm o **creștere bruscă a incidentelor fără intenții răuvoitoare**, deoarece pandemia de COVID-19 a devenit un multiplicator pentru **erorile umane** și **configurațiile greșite ale sistemului**, până la punctul în care majoritatea breșelor din 2020 au fost cauzate de erori.

Înțelegerea tendințelor legate de actorii care generează amenințări, de motivațiile și de țintele acestora ajută foarte mult la planificarea strategiilor de apărare și de atenuare a riscurilor în materie de securitate cibernetică. Aceasta este o parte integrantă a evaluării noastre globale a amenințărilor, deoarece permite să se acorde prioritate controalelor de securitate și să se elaboreze o strategie specifică pe baza impactului potențial și a probabilității de materializare a amenințărilor. Având în vedere acest lucru, în scopul ETL 2021, sunt luate în considerare următoarele patru categorii de actori care generează amenințări la adresa securității cibernetice:

- **Actori susținuți de stat**
- **Actori implicați în criminalitatea cibernetică**
- **Actori de tip hackeri de închiriat**
- **Hacktiviști**

Printr-o analiză continuă, ENISA a identificat tendințele și punctele de interes pentru fiecare dintre amenințările majore prezentate în ETL 2021. Principalele constatări și aprecieri din această evaluare se bazează pe resurse multiple și disponibile publicului, care sunt furnizate în referințele utilizate pentru elaborarea acestui document. Raportul se adresează în principal factorilor de decizie strategică și responsabililor de elaborarea politicilor, dar va fi, de asemenea, de interes pentru comunitatea tehnică din domeniul securității cibernetice.



PREZENTARE GENERALĂ A SITUAȚIEI AMENINȚĂRILOR

În cea de-a noua ediție a sa, raportul ENISA privind situația amenințărilor (ETL) oferă o prezentare generală a situației amenințărilor la adresa securității cibernetice. Raportul ETL este și strategic, și tehnic, conținând informații relevante atât pentru cititorii tehnici, cât și pentru cei non-tehnici. Activitatea din acest an a fost sprijinită de un grup de lucru ad-hoc nou format în cadrul ENISA pentru situația amenințărilor la adresa securității cibernetice[2].

Atacurile la adresa securității cibernetice au continuat să crească pe parcursul anilor 2020 și 2021, nu numai în ceea ce privește vectorii și numărul acestora, ci și în ceea ce privește impactul lor. Pandemia de COVID-19 a avut, de asemenea, un impact așteptat asupra situației amenințărilor la adresa securității cibernetice. Una dintre cele mai persistente evoluții care au rezultat în urma pandemiei de COVID-19 este trecerea de durată la un model de birou hibrid. Prin urmare, amenințările la adresa securității cibernetice legate de pandemie și de exploatarea „noii normalități" devin o obișnuință. Această tendință a mărit suprafața de atac și, prin urmare, am asistat la o creștere a numărului de atacuri cibernetice care vizează organizațiile și companiile prin intermediul birourilor de acasă[3].

În general, amenințările la adresa securității cibernetice au o tendință ascendentă. Stimulată de o prezență online din ce în ce mai mare, de tranziția infrastructurilor tradiționale către soluții online și bazate pe cloud, de interconectivitatea avansată și de exploatarea noilor caracteristici ale tehnologiilor emergente, cum ar fi inteligența artificială (IA)[4][5], situația securității cibernetice s-a dezvoltat în ceea ce privește gradul de sofisticare și de complexitate a atacurilor și impactul acestora. În special, amenințarea la adresa lanțurilor de aprovizionare și importanța acestora ca urmare a efectelor în cascadă, potențial catastrofale, a ajuns pe primul loc în rândul amenințărilor majore, determinând ENISA să elaboreze un raport privind situația amenințărilor dedicat acestei categorii de amenințări[6].

Trebuie remarcat faptul că, în această ediție a ETL, s-a acordat o atenție deosebită impactului amenințărilor cibernetice în diferite sectoare, inclusiv cele enumerate în Directiva privind securitatea rețelelor și a sistemelor informatice (Directiva NIS). Se pot obține informații interesante din particularitățile fiecărui sector în ceea ce privește situația amenințărilor, precum și din interdependențele potențiale și domeniile importante. În consecință, situația amenințărilor la nivel sectorial merită o atenție sporită.

De asemenea, în acest an s-au luat unele măsuri importante din partea apărătorilor din comunitatea cibernetică, precum și din partea responsabililor de elaborarea politicilor. Comunitatea globală a început să conștientizeze importanța comunicării și a cooperării în examinarea și urmărirea infractorilor cibernetici, în special ransomware-ul (cea mai importantă amenințare pentru perioada de raportare a ETL 2021) ocupând primul loc pe agendele reuniunilor privind strategia dintre liderii mondiali.

Cititorii consacrați ai edițiilor anterioare ale ETL 2021 vor observa o diferență în cartografierea amenințărilor principale. În acest an, ENISA a făcut un pas înapoi și a consolidat categoriile de amenințări, într-o acțiune care vizează integrarea și o mai bună reprezentare a amenințărilor similare. Acest lucru face parte din eforturile continue în vederea creării unei taxonomii restructurate a amenințărilor și va ajuta la stabilirea metodologică a tendințelor în următorii ani.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Cost of a Data Breach Report 2020 (Raport privind costul încălcării securității datelor 2020) - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA AI Threat Landscape (Raportul ENISA privind situația amenințărilor IA): https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISA Threat Landscape for Supply Chain Attacks (Raportul ENISA privind situația amenințărilor cu referire la atacurile care vizează lanțurile de aprovizionare), iulie 2021:https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Raportul ETL 2021 se bazează pe o varietate de informații din surse deschise și pe surse de informații privind amenințările cibernetice. Acest raport identifică principalele amenințări, tendințe și constatări și oferă strategii relevante de atenuare la nivel înalt. În prezent, ENISA lucrează la consolidarea metodologiei de raportare a situației amenințărilor, pentru a promova transparența și coerența activității.

1.1. PRINCIPALELE AMENINȚĂRI

În cursul anilor 2020 și 2021 au apărut și s-au materializat o serie de amenințări cibernetice. Pe baza analizei prezentate în acest raport, Raportul ENISA privind situația amenințărilor 2021 identifică și pune accent pe următoarele 8 grupe principale de amenințări (vezi Figura 1). Aceste 8 grupe de amenințări sunt evidențiate din cauza preponderenței lor în perioada de raportare, a popularității lor și a impactului pe care l-a avut materializarea acestora.

- **Ransomware (programe de șantaj digital)**
  Ransomware este un tip de atac rău-intenționat prin care atacatorii criptează datele unei organizații și cer o plată pentru a restabili accesul. Ransomware a fost principala amenințare în perioada de raportare, cu mai multe incidente cu impact mare și foarte mediatizate. Importanța și impactul amenințării de tip ransomware sunt evidențiate și de o serie de inițiative conexe în materie de politici în Uniunea Europeană (UE) și în întreaga lume.

- **Malware**
  Malware este un software sau firmware destinat să efectueze un proces neautorizat care va avea un impact negativ asupra confidențialității, integrității sau disponibilității unui sistem. Amenințarea reprezentată de programele malware a fost clasată în mod constant la un nivel ridicat timp de mulți ani, deși cu o tendință descendentă în perioada de raportare a ETL 2021. Utilizarea de noi tehnici de atac și unele victorii importante pentru comunitatea de aplicare a legii au avut un impact asupra operațiunilor actorilor relevanți care generează amenințări.

- **Criptojacking**
  Cryptojacking sau minarea ascunsă de criptomonedă este un tip de infracțiune cibernetică în care un infractor folosește în secret puterea de procesare a victimei pentru a genera criptomonedă. Odată cu proliferarea criptomonedelor și adoptarea lor tot mai extinsă de către publicul larg, s-a observat o creștere corespunzătoare a incidentelor la adresa securității cibernetice.

- **Amenințări legate de e-mail**
  Atacurile care vizează e-mailurile reprezintă un ansamblu de amenințări care exploatează mai degrabă punctele slabe ale psihicului uman și ale obiceiurilor de zi cu zi, decât vulnerabilitățile tehnice ale sistemelor informatice. În mod interesant și în ciuda numeroaselor campanii de sensibilizare și educare împotriva acestor tipuri de atacuri, amenințarea persistă în mare măsură. În special, compromiterea e-mailurilor de afaceri și tehnicile sofisticate avansate de extragere a câștigurilor monetare sunt în creștere.

- **Amenințări la adresa datelor**
  Această categorie cuprinde încălcarea securității datelor/scurgerile de date. Încălcarea securității datelor sau scurgerea de date reprezintă divulgarea de date sensibile, confidențiale sau protejate într-un mediu care nu este de încredere. Încălcarea securității datelor poate apărea ca urmare a unui atac cibernetic, a unei acțiuni din interior, a unei pierderi sau expuneri neintenționate de date. Amenințarea continuă să fie mare, deoarece accesul la date este ținta principală pentru atacatori din numeroase motive, de exemplu, extorcare, răscumpărare, defăimare, dezinformare etc.

- **Amenințări la adresa disponibilității și integrității**
  Disponibilitatea și integritatea sunt ținta unei multitudini de amenințări și atacuri, printre care se remarcă categoriile de atacuri de tip DoS (blocarea accesului) și atacurile web. Strict legat de atacurile bazate pe web, DDoS este una dintre cele mai grave amenințări la adresa sistemelor IT, vizând disponibilitatea acestora prin epuizarea resurselor, provocând scăderi de performanță, pierderi de date și întreruperi de servicii. Această amenințare ocupă în mod constant un loc important în Raportul ENISA privind situația amenințărilor, atât din cauza manifestării sale în incidente reale, cât și a potențialului său de impact mare.

- **Dezinformare - informare greșită**
  Campaniile de dezinformare și de informare greșită sunt în creștere, stimulate de utilizarea sporită a platformelor de comunicare socială și a mijloacelor de comunicare online, precum și ca urmare a creșterii prezenței online a persoanelor din cauza pandemiei de COVID-19. Este prima dată când acest grup de amenințări apare în raportul ETL; cu toate acestea, importanța sa în lumea cibernetică este mare. Campaniile de dezinformare și de informare greșită sunt utilizate frecvent în atacurile hibride pentru a reduce percepția generală de încredere, un promotor important al securității cibernetice.

- **Amenințări fără intenții răuvoitoare**
  Amenințările sunt considerate în mod obișnuit ca fiind activități voluntare și rău-intenționate ale unor adversari care atacă o anumită țintă conduși de anumite stimulente. Această categorie acoperă amenințările în care intenția răuvoitoare nu este evidentă. Aceste amenințări se bazează în principal pe erori umane și pe configurații greșite ale sistemului, dar se pot referi și la dezastre fizice care vizează infrastructurile IT. Și din cauza naturii lor, aceste amenințări au o prezență constantă în situația anuală a amenințărilor și reprezintă o preocupare majoră pentru evaluările de risc.

Figura 1: Raportul ENISA privind situația amenințărilor 2021 - Amenințări principale

Trebuie remarcat faptul că amenințările menționate mai sus implică categorii și grupuri de amenințări clasificate în funcție de cele opt domenii menționate mai sus. Fiecare dintre grupurile de amenințări este analizat în detaliu într-un capitol dedicat al prezentului raport, care detaliază particularitățile sale și oferă informații mai specifice, constatări, tendințe, tehnici de atac și vectori de atenuare.

1.2. TENDINȚE PRINCIPALE

Lista de mai jos rezumă principalele tendințe observate în situația amenințărilor cibernetice în perioada de raportare. Acestea sunt revizuite, de asemenea, în detaliu pe parcursul diferitelor capitole care alcătuiesc raportul ENISA din 2021 privind situația amenințărilor.

- S-au înmulțit **amenințările extrem de sofisticate și de impact care vizează lanțurile de aprovizionare**, după cum a evidențiat Raportul specific al ENISA privind situația amenințărilor care vizează lanțurile de aprovizionare. **Furnizorii de servicii gestionate** sunt ținte importante pentru infractorii cibernetici.
- **Pandemia de COVID-19 a impulsionat** atribuirea sarcinilor **de spionaj cibernetic** și a creat **oportunități pentru infractorii cibernetici.**
- **Organizațiile guvernamentale și-au intensificat activitatea în acest sens** atât la nivel național, cât și internațional. S-au observat eforturi intensificate din partea guvernelor de a-i perturba pe actorii susținuți de stat care generează amenințări și de a lua măsuri legale împotriva acestora.
- **Infractorii cibernetici sunt din ce în ce mai motivați de monetizarea** activităților lor, de exemplu, ransomware. **Criptomonedele** rămân cea mai frecventă metodă de plată pentru actorii care generează amenințări.
- Atacurile de criminalitate informatică **vizează și afectează din ce în ce mai mult infrastructura critică.**
- **Compromiterea prin intermediul e-mailurilor de phishing și atacul prin forță brută asupra serviciilor desktop la distanță (Remote Desktop Services – RDP)** rămân cei mai comuni doi **vectori ai infectării cu ransomware.**
- Accentul pus pe **modelele de afaceri de tip Ransomware as a Service (RaaS)** a crescut în 2021, ceea ce face dificilă atribuirea corectă a actorilor individuali care generează amenințări.
- Apariția schemelor de **ransomware cu extorcare triplă** a crescut puternic în cursul anului 2021.
- **Scăderea numărului de programe malware** care a fost observată în 2020 continuă și în cursul anului 2021. În 2021, am observat o creștere a numărului de actori care generează amenințări și care recurg la limbaje de programare relativ noi sau neobișnuite pentru a-și porta codul.
- **Programele malware care vizează mediile container** au devenit mult mai frecvente, cu evoluții noi, cum ar fi programele malware fără fișiere care sunt executate din memorie.
- Dezvoltatorii de programe malware continuă să găsească modalități **de a îngreuna ingineria inversă și analiza dinamică.**
- Volumul **infectărilor de tip cryptojacking** a atins un **nivel record** în primul trimestru al anului 2021, comparativ cu ultimii ani. **Câștigul financiar** asociat activității de cryptojacking i-a stimulat pe actorii care generează amenințări să efectueze aceste atacuri.
- **Volumul activităților de minare de criptomonedă în 2021 și de cryptojacking a atins un nivel record.**
- Putem observa că are loc o **trecere de la cryptojackingul bazat pe navigator la cel bazat pe fișiere**.
- **COVID-19 este în continuare momeala dominantă în campaniile** de atacuri prin e-mail.
- **Compromiterea e-mailului de afaceri (Business e-mail compromise - BEC)** s-a **intensificat** și a devenit un atac mai **sofisticat** și mai **țintit**.
- Modelul de afaceri **Phishing-as-a-Service (PhaaS)** câștigă teren.
- Actorii care generează amenințări și-au mutat atenția către **informațiile privind vaccinurile** în contextul amenințărilor la adresa securității datelor și informațiilor.
- S-a înregistrat o **creștere a numărului de încălcări ale securității datelor în sectorul sănătății**.
- Atacurile DDoS (Distributed Denial of Service) tradiționale se îndreaptă către **rețelele mobile și IoT (internetul lucrurilor)**.
- **Ransom Denial of Service (RDoS)** este noua frontieră a atacurilor care vizează blocarea accesului.
- **Partajarea resurselor în mediile virtualizate** acționează ca un amplificator al atacurilor DDoS.
- **Campaniile DDoS** din 2021 au devenit mai țintite, mult mai persistente și din ce în ce mai multivectoriale.
- **Dezinformarea facilitată de inteligența artificială (IA)** îi sprijină pe atacatori în desfășurarea atacurilor lor.
- **Activitatea de phishing se află în centrul atacurilor de dezinformare** și exploatează puternic convingerile oamenilor.
- **Informarea greșită și dezinformarea** se află în centrul activităților de criminalitate cibernetică și cresc într-un ritm fără precedent.
- **Modelul de afaceri Disinformation-as-a-Service (DaaS)** a crescut semnificativ, stimulat de impactul tot mai mare al pandemiei de COVID-19 și de nevoia de a dispune de mai multe informații.
- În 2020 și 2021, am observat o **creștere bruscă a incidentelor fără intenții răuvoitoare**, deoarece pandemia de COVID-19 a devenit un multiplicator pentru **erorile umane** și **configurațiile greșite ale sistemului**, până la punctul în care majoritatea breșelor din 2020 au fost cauzate de erori.

- S-a înregistrat o **creștere bruscă a incidentelor fără intenții răuvoitoare legate de securitatea în cloud**.

1.3. PROXIMITATEA PRINCIPALELOR AMENINȚĂRI FAȚĂ DE UE

Un aspect important care trebuie luat în considerare în contextul Raportului ENISA privind situația amenințărilor implică proximitatea unei amenințări cibernetice în raport cu Uniunea Europeană (UE). Acest aspect este deosebit de important pentru a-i ajuta pe analiști să evalueze importanța amenințărilor cibernetice, să le coreleze cu potențialii actori care generează amenințările și cu vectorii acestora și chiar să ghideze selectarea vectorilor de atenuare țintită corespunzători. În conformitate cu clasificarea propusă pentru politica europeană de securitate și apărare comună (PSAC)[7], clasificăm amenințările cibernetice în patru categorii, astfel cum sunt prezentate în Tabelul 1.

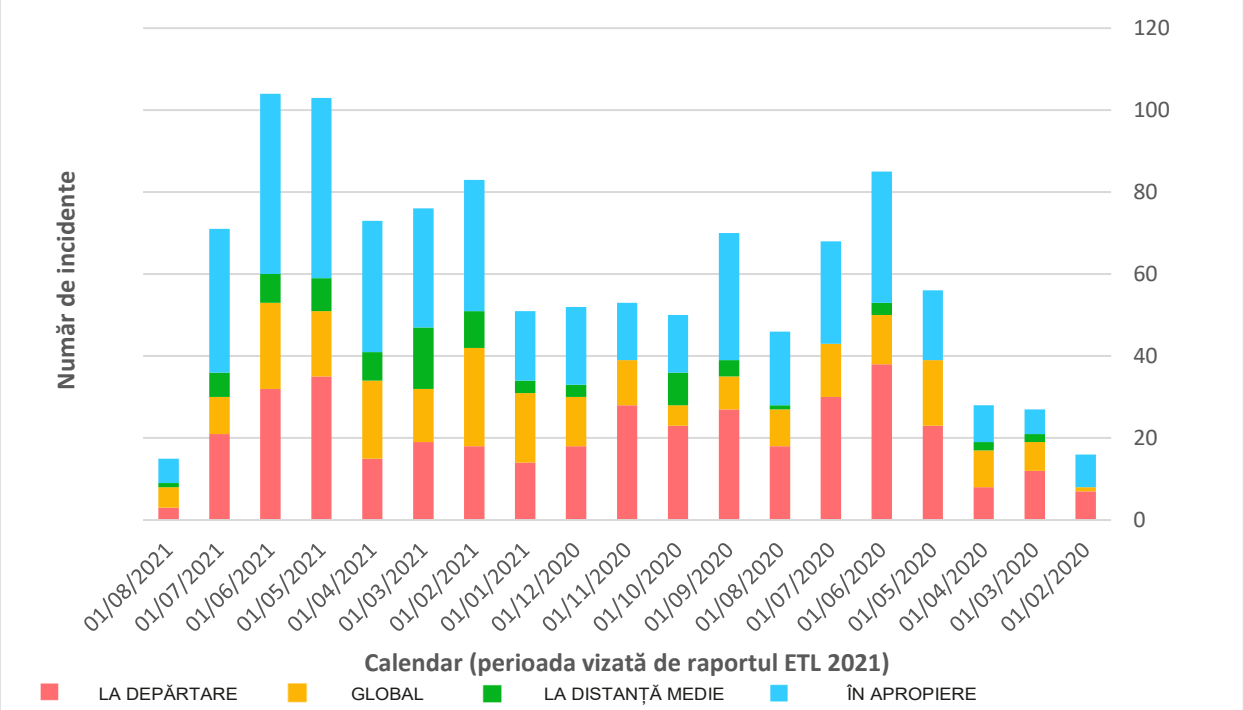
Tabelul 1: Clasificarea proximității amenințărilor cibernetice

Proximitate	Preocupări
ÎN APROPIERE	Rețele și sisteme afectate, controlate și asigurate în interiorul frontierelor UE. Populația afectată în interiorul frontierelor UE.
LA DISTANȚĂ MEDIE	Rețele și sisteme considerate vitale pentru obiectivele operaționale în cadrul domeniului de aplicare al pieței unice digitale a UE și al sectoarelor reglementate de Directiva NIS, dar controlul și asigurarea acestora sunt în sarcina autorităților instituționale din afara UE sau a autorităților publice sau private din statele membre. Populația afectată din zonele geografice din apropierea frontierelor UE.
LA DEPĂRTARE	Rețele și sisteme care, dacă sunt influențate, vor avea un impact critic asupra obiectivelor operaționale în cadrul domeniului de aplicare al pieței unice digitale a UE și al sectoarelor reglementate de Directiva NIS. Controlul și asigurarea acestor rețele și sisteme ies din sfera de competență a autorităților instituționale ale UE sau a autorităților publice sau private ale statelor membre. Populația afectată din zonele geografice la mare distanță de UE.
GLOBAL	Toate zonele menționate mai sus.

Figura 2 prezintă calendarul incidentelor legate de principalele categorii de amenințări raportate în ETL 2021. Trebuie precizat faptul că informațiile din grafic se bazează pe OSINT (informații din surse deschise) și sunt rezultatul activității desfășurate de ENISA în domeniul conștientizării situației[8].

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] În conformitate cu Regulamentul UE privind securitatea cibernetică, articolul 7, alineatul (6) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Figura 2: Calendarul incidentelor observate în legătură cu principalele amenințări menționate de raportul ETL (conștientizarea situației pe baza OSINT) în funcție de proximitatea acestora.



După cum reiese din figura de mai sus, în 2021 s-a înregistrat un număr mai mare de incidente în comparație cu 2020. În special, categoria ÎN APROPIERE are un număr care crește constant de incidente observate legate de amenințările principale, ceea ce implică importanța acestora în contextul UE. În mod nesurprinzător, tendințele lunare (care nu sunt prezentate în figură din motive de concizie) sunt destul de similare între diferitele categorii, deoarece securitatea cibernetică nu cunoaște frontiere și, în majoritatea cazurilor, amenințările se materializează la toate nivelurile de proximitate. Trebuie remarcat faptul că, în ultimele luni acoperite de raportul ETL 2021, se observă o proximitate mai mare în raportul UE-ÎN APROPIERE, o tendință pe care ENISA va continua să o monitorizeze pentru a vedea evoluția sa și ce legătură are cu activitățile actorilor care generează amenințări și cu vectorii de amenințare în curs.

1.4. AMENINȚĂRILE PRINCIPALE PENTRU FIECARE SECTOR

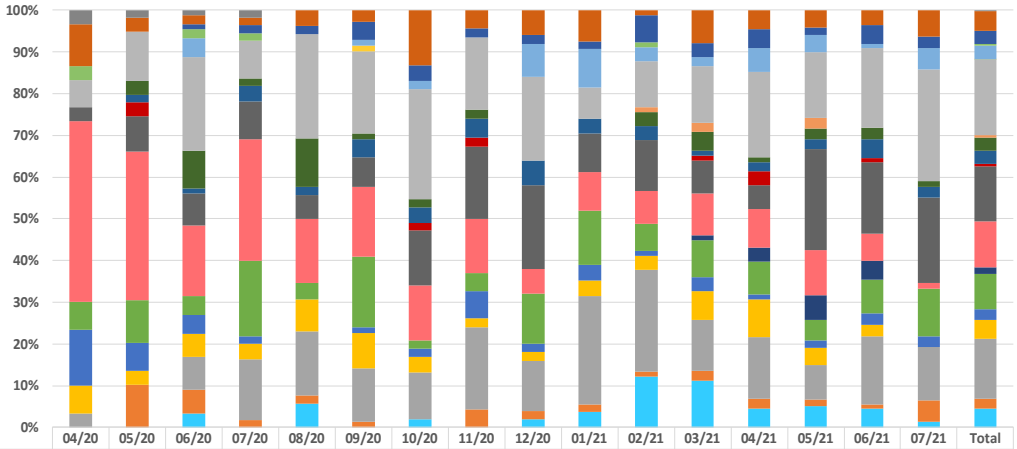
Amenințările cibernetice nu se limitează, de obicei, la un anumit sector și, în cele mai multe cazuri, afectează mai multe dintre acestea. Acest lucru este adevărat, deoarece, în multe cazuri, amenințările se manifestă prin exploatarea vulnerabilităților din sistemele TIC subiacente care sunt utilizate într-o varietate de sectoare. Cu toate acestea, atacurile țintite, precum și atacurile care exploatează diferențele de maturitate în materie de securitate cibernetică dintre sectoare și popularitatea/importanța anumitor sectoare sunt factori care trebuie luați în considerare. Acești factori contribuie la manifestarea amenințărilor ca incidente în anumite sectoare și, de aceea, este important să se analizeze în profunzime aspectele sectoriale ale incidentelor și amenințărilor observate. În plus, tendințele sesizate în fiecare sector și dependențele intersectoriale sunt observații care pot rezulta dintr-o astfel de analiză.

Figurile 3 și 4 evidențiază sectoarele afectate cu privire la incidentele observate pe baza OSINT (informații din surse deschise) și sunt rezultatul activității desfășurate de ENISA în domeniul conștientizării situației[9]. Acestea se referă la incidente legate de principalele amenințări din raportul ETL 2021. Aceasta este prima încercare a ENISA de a cartografia impactul amenințărilor asupra unor sectoare specifice. În anii următori și în viitoarele ediții ale situației

[9] În conformitate cu Regulamentul UE privind securitatea cibernetică, articolul 7, alineatul (6) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

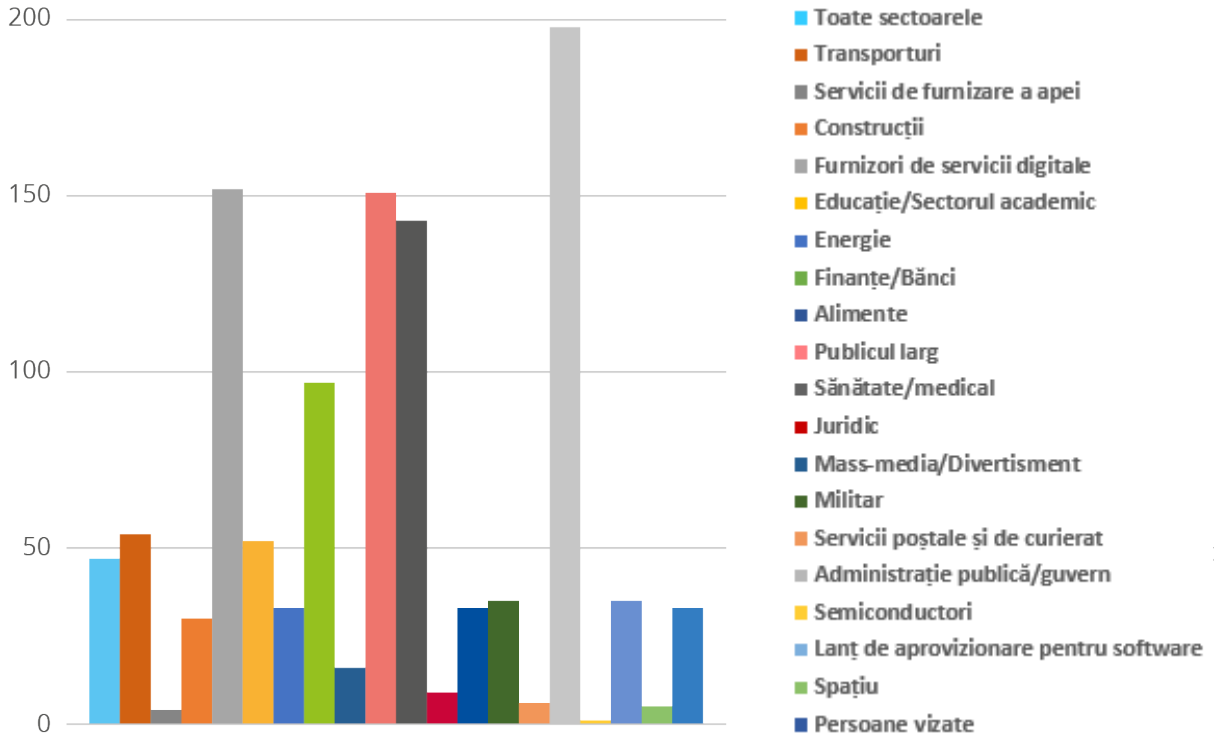
amenințărilor, se vor depune eforturi pentru a alinia sectoarele la cele enumerate în Directiva privind securitatea rețelelor și a sistemelor informatice (Directiva NIS) și în propunerea de revizuire a acesteia (NIS 2).

Figura 3: Calendarul incidentelor observate în legătură cu principalele amenințări din raportul ETL în funcție de sectorul afectat.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Total
Servicii de furnizare a apei	1	1	1	1													2
Transporturi	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Persoane vizate			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Spațiu	1		2	1							1						4
Lanț de aprovizionare pentru software			4			1	1		4	5	3	2	5	5	1	4	35
Semiconductori						1											1
Administrație publică/guvern	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Servicii poștale și de curierat											1	2		3			6
Militar		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Mass-media/Divertisment		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Juridic		2					1	1				1	3		1		7
Sănătate/medical	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Publicul larg	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Alimente												1	3	7	5		16
Finanțe/Bănci	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energie	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Educație/Sectorul academic	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Furnizori de servicii digitale	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Construcții		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Toate sectoarele			3		3		1		1	2	11	10	4	6	5	1	47

Figura 4: Sectoarele vizate în funcție de numărul de incidente (aprilie 2020-iulie 2021)



În această perioadă de raportare, un număr mare de incidente au vizat administrația publică și guvernul și furnizorii de servicii digitale. Era de așteptat ca aceștia din urmă să reprezinte ținte, având în vedere furnizarea orizontală de servicii pentru acest sector și, prin urmare, impactul său asupra multor alte sectoare. Am observat, de asemenea, un număr semnificativ de incidente care au vizat utilizatorii finali și nu neapărat un anumit sector. Sectorul sănătății a fost, de asemenea, vizat în mod semnificativ, iar această activitate dă semne de creștere în ultimele luni ale perioadei de raportare (mai-iulie 2021). Este interesant faptul că sectorul financiar se confruntă cu un număr constant de incidente pe tot parcursul anului. Lanțul de aprovizionare pentru software prezintă, de asemenea, o creștere a numărului de incidente în cursul anului 2021, reprezentând și aceasta o observație din raportul ENISA privind situația amenințărilor care vizează lanțurile de aprovizionare[10].

1.5. METODOLOGIE

Raportul ENISA privind situația amenințărilor (ETL) 2021 se bazează pe informații disponibile din surse deschise, în principal de natură strategică, și pe capacitățile proprii de informații privind amenințările cibernetice ale ENISA și acoperă mai multe sectoare, tehnologii și contexte. Raportul urmărește să fie nepărtinitor în raport cu industria și furnizorii și face referiri sau citează lucrări din diverse cercetări în domeniul securității, bloguri din domeniul securității și articole din mass-media, identificate în text în mai multe note de subsol. Intervalul de timp vizat de raportul ETL 2021 este cuprins între aprilie 2020 și iulie 2021 și este denumit „perioada de raportare” în întregul raport.

Pentru realizarea raportului ETL 2021 s-a utilizat următoarea abordare. Pe parcursul întregii perioade de timp relevante, ENISA, prin conștientizarea situației, a adunat o listă de incidente majore, așa cum au apărut în surse deschise. Această listă a servit ca bază pentru identificarea listei de amenințări principale, precum și ca material sursă pentru mai multe tendințe și statistici din raport.

[10] ENISA Threat Landscape for Supply Chain Attacks (Raportul ENISA privind situația amenințărilor cu referire la atacurile care vizează lanțurile de aprovizionare), iulie 2021: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Ulterior, ENISA și experți externi au efectuat cercetări documentare detaliate ale literaturii disponibile din surse deschise, cum ar fi articole de presă, opinii ale experților, rapoarte de date operative, analize ale incidentelor și rapoarte de cercetare în domeniul securității. Printr-o analiză continuă, ENISA a identificat tendințele și punctele de interes pentru fiecare dintre amenințările majore prezentate în raportul ETL 2021. Principalele constatări și aprecieri din această evaluare se bazează pe resurse multiple și disponibile publicului, care sunt furnizate în referințele utilizate pentru elaborarea acestui document.

În cadrul raportului, încercăm să facem diferența între ceea ce a fost raportat de sursele noastre și ceea ce reprezintă evaluarea noastră. (Facem acest lucru utilizând în mod specific expresia „conform evaluării noastre"). În cele din urmă, atunci când efectuăm o evaluare, transmitem ideea de probabilitate prin utilizarea unor cuvinte care exprimă o estimare a probabilității (de exemplu, probabil, foarte probabil, cu siguranță)[11].

Cadrul MITRE ATT&CK®[12] a fost utilizat în prezentul raport pentru a evidenția tacticile și tehnicile de atac relevante pentru o amenințare dată (vezi anexa A). Pentru fiecare tactică ATT&CK® sunt prezentate tehnicile folosite de adversar. Acest lucru poate avea ca rezultat o listă de măsuri de atenuare ATT&CK[13] care pot fi aplicate. MITRE ATT&CK® este o bază de cunoștințe, un limbaj comun privind tacticile și tehnicile adversarului pe baza observării realității. Baza de cunoștințe MITRE ATT&CK® este utilizată ca bază pentru dezvoltarea de modele și metodologii specifice legate de amenințări în sectorul privat, în sectorul guvernamental și în comunitatea de produse și servicii pentru securitatea cibernetică.

Raportul a fost validat de Grupul de lucru ad-hoc al ENISA privind situația amenințărilor cibernetice[14], care a fost înființat în aprilie 2021, un grup format din experți ai organismelor europene și internaționale din sectorul public și cel privat.

Pentru elaborarea în viitor a rapoartelor privind situația amenințărilor, ENISA este în curs de formalizare a unei noi metodologii, pentru a promova transparența și a pune bazele unor procese structurate și bine aliniate. În cadrul acestui efort, împreună cu o taxonomie revizuită a amenințărilor, metodologia pentru rapoartele privind situația amenințărilor va fi făcută publică în viitor.

1.6. STRUCTURA RAPORTULUI

Raportul ENISA privind situația amenințărilor (ETL) 2021 a păstrat structura rapoartelor ETL anterioare, utilizând o structură similară pentru a evidenția principalele amenințări cibernetice în 2021. Cititorii edițiilor anterioare vor remarca faptul că categoriile de amenințări au fost consolidate în conformitate cu trecerea la o nouă taxonomie a amenințărilor la adresa securității cibernetice care va fi utilizată în viitor.

Prezentul raport are următoarea structură:

Capitolul 2 explorează tendințele legate de actorii care generează amenințări (adică actori susținuți de stat, actori din domeniul criminalității cibernetice, actori de tip hackeri de închiriat și hacktiviști).
Capitolul 3 ia în discuție principalele constatări, incidente și tendințe în ceea ce privește activitățile de tip ransomware.
Capitolul 4 prezintă principalele constatări, incidente și tendințe în ceea ce privește activitățile de tip malware.
Capitolul 5 descrie principalele constatări, incidente și tendințe în ceea ce privește activitățile de tip cryptojacking.
Capitolul 6 evidențiază principalele constatări, incidente și tendințe în ceea ce privește amenințările la adresa e-mailului.
Capitolul 7 ia în discuție principalele constatări, incidente și tendințe în ceea ce privește amenințările la adresa securității datelor.
Capitolul 8 prezintă principalele constatări, incidente și tendințe în ceea ce privește amenințările la adresa disponibilității și integrității.

[11] CIA - Words of Estimative Probability (Cuvinte pentru estimarea probabilității)
https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

Capitolul 9 subliniază importanța amenințărilor hibride și descrie principalele constatări, incidente și tendințe privind dezinformarea și informarea greșită.
Capitolul 10 pune accentul pe principalele constatări, incidente și tendințe în ceea ce privește amenințările fără intenții răuvoitoare.
Anexa A prezintă tehnicile utilizate în mod obișnuit pentru fiecare amenințare, pe baza cadrului MITRE ATT&CK®.
Anexa B include incidentele semnificative pentru fiecare amenințare, așa cum au fost observate în perioada de raportare.