Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

Transmiterea și protejarea informațiilor în mediul public digital

- lucrare de licență, Administrație Europeană-

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Diaconescu Alexandru-Nicolae

București
2023

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarația anti-plagiat și nici instrucțiunile** – acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile / Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development: https://scrd.eu/index.php/spr/index.

ATENȚIE: Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat

1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice).
2. Declar că nu am permis și nu voi permite nimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.

3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.

Numele și prenumele: Diaconescu Alexandru-Nicolae

Data și semnătura: 24.05.2023 

Cuprins

Listă de abrevieri folosite în elaborarea lucrării:

- SIM- Subscriber Identity Module
- ATM- Automated Teller Machine
- SIM- Subscriber Identity Module
- UE- Uniunea Europeană
- ARPANET- Advanced Research Projects Agency Network
- NASA- National Aeronautics and Space Administration
- FBI- Federal Bureau of Investigation
- AOL- America Online
- DDoS- Distributed Denial of Service
- CIA- Central Intelligence Agency
- PLC- Programmable Logic Controller
- USB- Universal Serial Bus
- SO- Sistem de operare
- PIN- Personal Identification Number
- P2P- Peer-to-peer
- GIF- Graphics Interchange Format
- RAM- Random Access Memory
- MBR- Master Boot Record
- BS- Boot Sector
- CD- Compact Disk
- DVD- Digital Video Disc
- VBA- Visual Basic for Applications
- IRC- Internet Relay Chat
- USD- dolari americani
- EUR- euro
- SMB- Server Message Block
- NHS- National Health Service
- TSB- The Shadow Brokers

Abstract

Lucrarea elaborată are ca scop aprofundarea și explicarea metodelor prin care informațiile sunt transmise și protejate în mediul public digital. Obiectivele acesteia sunt reprezentate de o mai bună înțelegere a modului în care informațiile sunt protejate prin intermediul criptării și a cheilor de criptare folosite în mediul public digital dar și principalele vulnerabilități ce apar în procesul de stocare și transmitere a informațiilor. Lucrarea este bazată pe diverse cercetări din domeniul securității datelor, lucrări ce aparțin atât cercetătorilor români cât și celor americani sau indieni. Conceptele ce fundamentează studiul sunt securizarea datelor prin intermediul criptării informației și atacurile cibernetice care vizează informația din mediul public digital. Abordarea folosită pentru a descrie cercetarea este de tip cantitativ, la baza acesteia fiind un chestionar realizat asupra unui eșantion format din persoane de diferite vârste cu privire la încrederea pe care subiecții o au în privința securității datelor din mediul publc digital. Studiul are ca implicații creșterea gradului de conștientizare asupra importanței securității informației din mediul public digital, al analizei și al elaborării de noi metode pentru a preveni atacurile cibernetice dar și de a evidenția vulnerabilitățile care apar în procesul de transmitere al informațiilor din mediul public digital. Contribuția personală adusă asupra lucrării este oferită de manieră în care cumulul de informații și date oferite de studiile anterior efectuate sunt concretizate și structurate în vederea punerii în evidență a importanței temei alese. Lucrarea elaborată este de un înalt nivel al calității datorită implicării numeroaselor surse de documentare provenite din diverse părți ale lumii ce stau la baza realizării acesteia, având un caracter original și note personale ce sunt menite să descrie în detaliu tema aleasă.

Cuvinte cheie: criptare, atacuri cibernetice, tehnici de criptare, vulnerabilități

Introducere

Importanța studierii metodelor prin care informația este transmisă și protejată în mediul public digital este evidențiată prin numeroase studii, sondaje, cărți, dezbateri și al altor modele teoretice. În era tehnologizării și a online-ului informația este puterea, o putere ce nu poate fi lăsată în mâna oricui. Încă din cele mai vechi timpuri, au existat forme de administrație publică ce aveau ca scop stabilirea unei ordini și al bunului mers al lucrurilor în societate. Pentru ca administrația publică să funcționeze într-un mod cât mai eficient, aceasta are la baza informații și date primite de la cetățeni. Ce s-ar întâmpla dacă toate aceste informații ar ajunge la persoane rău intenționate? Cu siguranță urmările nu ar fi deloc unele favorabile atât pentru cetățeni cât și pentru administrația publică. Astfel, studiul realizat asupra transmiterii și protejării informațiilor în mediul public digital își dorește să reafirme importanța protejării informației și să explice metodele prin care aceasta este securizată. Cercetarea are la bază lucrări ale experților în domeniu din diferite părți ale globului cum ar fi: Statele Unite ale Americii, India, Marea Britanie, Elveția dar și ai unor profesori și scriitori din Moldova- profesorul Aureliu Zgureanu- și nu în cele din urmă profesorul coordonator al acestei lucrări: Conf. Univ. Dr. Cătălin Vrabie.

În prima parte, cercetarea realizată se bazează atât pe lucrările și cercetările anterior realizate de către experți în domeniul securității informației dar și pe o explicare mai clară a modului în care informația este protejată prin intermediul criptării, istoria criptării informațiilor și la final, realizarea și interpretarea unui sondaj pentru a arăta nivelul de încredere al populației în ceea ce privește protecția informațiilor în mediul public digital. În cea de-a doua parte a lucrării, sunt analizate atacurile cibernetice pornind de la definirea acestora, prezentarea tipurilor de atacuri cibernetice, principalele vulnerabiltăți ale sistemelor și cum pot fi prevenite aceste atacuri. Capitolul 3 este dedicat studiului de caz ce analizează un caz real al unui atac de tip Ransomware asupra unor dispozitive utilizate în mediul public digital pentru a demonstra care sunt consecințele unei slabe protecții în fața atacurilor cibernetice.

Context

Contextul studiului de caz este oferit de pericolul iminent la care utilizatorii mediului digital se supun atunci când utilizează dispozitive și programe ce nu sunt sigure. În plus, studiul de caz vine ca o completare a primelor două capitole, îmbinând astfel modul în care datele sunt criptate în cazul atacurilor de tip ransomware cât și informații privind un caz concret al unui atac de acest tip.

Capitolul 1. Cum sunt protejate informațiile?

1.1. Ce este criptografia?

Primul subcapitol al acestei cercetări are ca scop introducerea într-un mod cât mai simplu și ușor de înțeles a noțiunilor de bază despre criptografie dar și a criptanalizei. În începutul acestuia vom răspunde la întrebări simple precum ,,Ce este criptografia?", ,,Care sunt obiectivele criptografiei?", ,,Ce este criptanaliza?", ,,De ce este importantă criptarea informației și ce rol are aceasta în protecția informațiilor?". Continuarea răspunsurilor la aceste întrebări este reprezentată de introducerea unor definiții și a unor termeni de specialitate din domeniul criptografiei. De asemenea, vom vorbi despre obiectivele principale ale criptografiei și despre cum criptografia este întâlnită în viața cotidiană.

Criptografia este ramura matematicii ce are ca scop securizarea informației dar și autentificarea și restricționarea accesului la informație într-un sistem informatic. Termenul de ,,criptografie" provine din limba greacă și este format prin alăturarea cuvintelor kryptós (ascuns) și gráfein (a scrie), astfel termenul de criptografie având ca traducere ,,a scrie ascuns". În realizarea procesului de criptare a informației sunt utilizate în principal metode matematice a căror complexitate de rezolvare este suficient de înaltă pentru a păstra informația în siguranță. Criptografia are patru obiective principale:

- Confidențialitatea (sau în limba engleză privacy) – reprezintă proprietatea de a păstra secretul informației în vederea utilizării acesteia doar de către persoanele autorizate.
- Integritatea datelor – reprezintă proprietatea de a evita orice modificare neautorizată a informațiilor (ștergere, inserare, substituție).
- Autentificarea – reprezintă proprietatea de a identifica o entitate în urma analizării unor criterii de securitate.
- Non-repudierea – reprezintă proprietatea care previne negarea unor evenimente anterioare. [1]

Din cele patru obiective menționate mai sus derivă și alte obiective legate de securitatea informației precum:

- Revocarea – retragerea unui drept;
- Certificarea – dovedirea autenticității;
- Autorizarea – împuternicirea sau obținerea unui drept;
- Validarea – recunoașterea valabilității;
- Semnături – asocierea de informații unei entități;
- Autentificarea mesajelor - identificarea mesajelor, a sursei;
- Autentificarea entităților – identificarea entităților;
- Controlul accesului – accesul selectiv la resurse;
- Anonimitatea – lipsa identificării unei entități sau mesaj;
- Datarea – (în engleză timestamping) stabilirea datei exacte a unui eveniment.

Criptografia este întâlnită în aproape orice sistem de comunicație folosit în zilele noastre. Dincolo de sistemele informatice, rețele de calculatoare sau orice alte mijloace de comunicare, criptarea este folosită și în acțiuni de zi cu zi precum: tranzacțiile online pentru cumpărături, mesaje transmise prin intermediul rețelelor de internet, folosirea cardului bancar cu CIP[1] în ATM-uri[2] sau la plățile din magazine, telecomanda pentru blocarea/deblocarea mașinii, cartelele SIM[3] ale telefoanelor mobile etc.

[1] CIP- acronim pentru Centrala Incidentelor de Plăți (CIP) este o structură specializată în colectarea, păstrarea și gestionarea datelor specifice despre incidentele de plăți care au avut loc cu titularii de cont care folosesc cecuri, cambii și bilete la ordin. [50]

[2] ATM- acronim provenit din denumirea în engleză „Automated Teller Machine". Este un automat bancar la care se pot realiza tranzacții.

[3] SIM- acronim pentru Subscriber Identity Module, este un card de memorie de mici dimensiuni folosit pentru a face posibilă utilizarea serviciilor unui operator de telefonie mobilă.

O altă ramură a matematicii ce se află într-o strânsă legătură cu Criptografia este Criptanaliza. Termenul de Criptanaliza provine tot din limba greacă și este format din alăturarea cuvântului kryptós (ascuns) și al cuvântului analýein (a dezlega). Astfel, Criptanaliza este ramura matematicii ce se ocupă cu studiul metodelor de obținere a înțelesului informației criptate [1], cu mențiunea că acest process are loc fără a avea acces la informația criptată.
Cele două ramuri ale matematicii prezentate mai sus constituie împreună Criptologia, termen ce provine tot din limba greacă de la cuvintele kryptós (ascuns) și λόγος (cuvânt). Criptologia este astfel știința care se ocupă cu procesele de criptare și decriptare a informației.

Criptarea este procesul de conversie a textului simplu în text criptat. Criptarea este una din cele mai importante părți ale criptografiei, dar nu cuprinde întreaga știință. Principalul aspect al procesului de criptare este reprezentat de prezența atât a unui algoritm cât și a unei chei de criptare. [2] Algoritmul criptografic, cunoscut și sub numele de cifru (cipher în limba engleză), este o funcție matematică ce este folosită în procesul de criptare/decriptare a informației. Cheia de criptare este la rândul său tot o informație cu rolul de a specifica modul în care asupra textului simplu a fost aplicat algoritmul de criptare. Această cheie este folosită pentru a cripta un text clar și este de exemplu un cuvânt, o frază, un text mai lung sau un număr. În lipsa acestei chei de criptare, decriptarea unei informații este dificilă sau chiar imposibil de realizat chiar dacă metoda de criptare este cunoscută. Chiar dacă algoritmul aplicat unui text clar este identic, utilizarea unei chei de criptare diferite duce la obținerea unui text codificat diferit. Confidențialitatea mesajului criptat este direct proporțională cu puterea și complexitatea algoritmului de criptare dar și a confidențialității cheii de criptare. [3]

1.2. Evoluția criptării informației

Criptografia, cunoscută și ca arta scrierii cifrate și a dezlegării codurilor, are o istorie lungă și bogată ce datează de mii de ani. Această știință este folosită încă de pe vremea popoarelor egiptene, a celor greceşti și a celor romane, cu scopul de a proteja informațiile sensibile din a fi citite și înțelese de persoane nedorite. Egiptenii se foloseau de un sistem bazat pe hieroglife pentru a face înscrieri pe pereții mormintelor și a sarcofagelor. De altfel, hieroglifele sunt întâlnite și pe unele obiective precum coloanele egiptene ce poartă numele de obeliscuri. În Grecia antică, spartanii utilizau bucăți lungi de piele pe care le înfășurau în jurul unor bețe. Înfășurate pe aceste bețe, informațiile nu aveau sens, însă odată ce erau desfășurate ele puteau fi descifrate datorită diametrului bățului în jurul căreia erau înfășurate. În Roma antică, împăratul Julius Caesar utiliza o modalitate de criptare a informațiilor bazată pe o substituire simplă a literelor. Astfel, fiecare literă din alfabet era schimbată cu o alta, existând un număr exact de poziții în urma căreia substituția era realizată. În acest fel, mesajele trimise de împăratul Julius Caesar puteau să fie citite doar de către persoanele ce cunoșteau acest algoritm. Această metodă de criptare a informațiilor a fost folosită timp de secole ea fiind cunoscută și sub numele de ,,Cifrul lui Caesar". Cifrul lui Caesar (fig. 1) a fost unul din primele cifruri cu substituție, algoritmul pe care acesta se baza era prin substituția literelor cu o altă literă aflată la 3 poziții distanță în alfabet. Se presupune că el a fost utilizat în comunicarea dintre împăratul Julius Caesar și generalii armatelor sale în timpul campaniilor militare. [4]

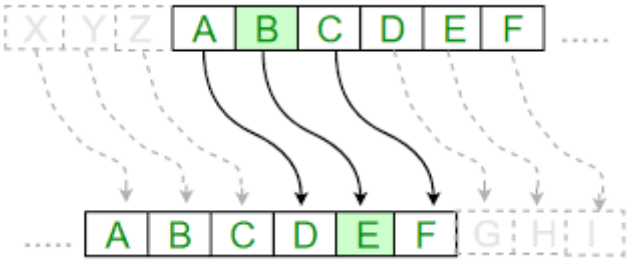


Fig. 1 Cifrul lui Caesar
Sursa: https://www.invata-programare.ro/article/cifru-de-tip-caesar

Sute de ani mai târziu, în Italia secolului al XV-lea, a fost creat un sistem ingenios de criptare a informațiilor de către Leon Battista Alberti. Sistemul avea forma unui disc pe care se găseau

două rânduri de litere și o parte mobilă. Acest disc a fost creat pentru a cripta și a decripta mesajele fie prin lăsarea părții mobile în aceeași poziție (astfel rezultând cifrul monalfabetic) fie prin deplasarea periodică a părții mobile (rezultând cifrul polialfabetic). Criptarea polialfabetică folosește substituția simbolului inițial cu un șir de alte simboluri. În anul 1518 a apărut prima carte ce avea ca temă criptologia și anume ,,Poligraphiae libri sex". În această carte era descrisă o metodă de criptare ce purta denumirea de tablou de transpoziție. Cifrul lui Leon Battista Alberti a fost urmat de un alt cifru polialfabetic inventat de Johannes Trithemius în anul 1518. Noul cifru purta denumirea de tabula recta (fig. 2) și reprezenta un pătrat format din mai multe alfabete în care fiecare linie era decalată cu un loc spre stânga față de linia precedentă. Acest cifru, asemeni cifrului creat de Leon Battista Alberti și al tuturor cifrurilor polialfabetice are la bază cifrul Caesar.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 2 Tabula Recta
Sursa: https://www.descopera.ro/cultura/10056537-criptografia-si-codurile-secrete-care-au-marcat-istoria

În anul 1553, Giovan Battista Bellaso avea să inventeze cifrul Vigenère pe care l-a descries în propria sa carte intitulată „La cifra del. Sig. Giovan Battista Bellaso". Asemeni cifrelor anterior menționate la baza acestuia stă tot o serie de cifruri Caesar diferite, fiind o formă simplă de substituție polialfabetică. Cunoscut și ca ,,le chiffre indéchiffrable" (tradus din franceză ca cifrul indescifrabil) el a fost asociat greșit în secolul al XIX-lea unui francez pe nume Blaise de Vigenère de unde a primit și numele de ,,Cifrul Vigenère". Denumirea de cifrul indescifrabil se datorează aparențelor pe care acesta le prezintă în fața începătorilor în arta decriptării: este un cifru ușor de înțeles și implementat dar care pare imposibil de spart pentru un începător. [5]

Lucrarea intitulată ,,De rerum varietate" scrisă de matematicianul și medicul italian Gerolamo Cardano a prezentat lumii viziunea lui pentru întărirea siguranței informației criptate prin schimbarea cheii la fiecare mesaj. Această idee consta în folosirea mesajului însuși drept cheie de decriptare a informației. Metoda presupunea o grilă ce conținea un număr de ferestre la intervale neregulate ce aveau o lungime variabilă și înălțimea unui rând de scris. După ce grila era așezată pe hârtia pe care se afla textul, mesajul secret se scria în ferestre iar pentru a fi descifrat era necesar ca grila să fie reașezată deasupra textului primit. Acest proces era unul greoi, motiv pentru care Cardano a modificat procesul prin înlocuirea inserției textului în clar după o regulă specifică în pătratele ce se aflau la rândul lor într-un pătrat ce avea aceeași dimensiune ca și grila folosită cu o transpoziție realizată prin rotirea grilei. Această modalitate era considerată ca fiind o formă primară a metodelor de transpoziție.

Criptografia a jucat un rol extrem de important și în cazul bătăliilor purtate de regii Franței în secolul al XVII-lea. Cu ajutorul criptografiei și al criptologului francez Antoine Rossignol, regii Ludovic al XIII-lea și Ludovic al XIV-lea au obținut numeroase victorii în luptele purtate, un exemplu ar fi Asediul La Rochelle unde Antoine Rossignol a reușit să descifreze mesajele pe care hughenoții asediați de trupele franceze au încercat să le transmită. Astfel, Rossignol a devenit primul criptolog profesionist din Franța, considerat a fi cel mai abil criptolog din Europa acelei vremi. De asemenea, el și-a adus aportul și în ceea ce privește relațiile diplomatice,

corespondența diplomatică nefiind un secret pentru acesta. Principala sa realizare a fost modificarea modului de stabilire a corespondenței dintre elementele clare ale mesajului și cifruri, astfel ducând la introducerea a două noi tipuri de corespondențe denumite tabel de cifrare respectiv tabel de descifrare.

În epoca modernă, criptologia a avut parte de o dezvoltare semnificativă odată cu inventarea telegrafului. Datorită dezvoltării societății, a industriei și a comerțului nevoia de comunicare a crescut, ducând astfel la apariția telegrafului ce avea ca scop facilitarea comunicațiilor. Dincolo de componenta civilă a acestuia, telegraful a fost utilizat intens și în cadrul comandamentelor militare atât prin intermediul unei mai bune comunicări între bazele militare cât și în cadrul operațiunilor militare desfășurate de către acestea. Acest lucru a făcut posibil controlul permanent al acțiunilor militare și creșterea cantității de informație secretă ce putea fi transmisă. Un alt reper în dezvoltarea criptării și al transmiterii de informații criptate a fost reprezentat de apariția radioului. În timpul primului război mondial radioul a fost folosit ca mijloc de transmitere a informațiilor secrete (informații clasificate de natură militară) dar și a informațiilor ce țin de sfera diplomației. Astfel a crescut exponențial cantitatea de informație fapt ce a avut ca o consecință secundară creșterea interesului pentru criptanaliză. Acest lucru s-a datorat dorinței de a intercepta și a decripta mesajele trimise de către inamici pe frontul de luptă. La începutul anilor 1920 a fost dezvoltată o nouă metodă de criftografie ce avea ca scop protejarea mesajelor diplomatice. Tehnica consta în utilizarea unor ,,blocuri cu o singură utilizare", așa cum a fost această metodă cunoscută. Blocurile erau formate din cifre aleatorii (grupate sub forma unor grupuri) ce mai apoi erau tipărite și legate într-o carte. Secretul acestei metode consta în utilizarea unică a fiecărei foi (după ce erau folosite acestea erau aruncate). Chiar dacă metoda a fost dezvoltată în cel mai mare secret, ea a sfârșit prin a fi răspândită în întreaga lume în mai puțin de 15 ani. Chiar și în ziua de astăzi această tehnică de criptare este cunoscută ca fiind una din cele mai sigur metode criptografice și este folosită în continuare. [6]

În timpul celui de-al doilea război mondial apare o altă mașinărie ce avea să își pună amprenta puternic în istoria criptografiei și anume apariția mașinăriei Enigma (fig. 3). Această mașinărie a fost folosită de armata Germaniei naziste în timpul celui de-al doilea război mondial în vederea transmiterii de mesaje criptate. Armata Aliaților a reușit să decripteze un număr crescut de mesaje cu ajutorul criptografilor polonezi Marian Rejewski, Jerzy Rozycky și Henryk Zygalski. Aceștia au împărtășit cu Franța și Regatul Unit tehnica de decriptare și de reconstrucție a mesajelor ceea ce a dus la un avantaj considerabil pentru armata Aliaților în fața Germaniei naziste. Descifrarea informațiilor a fost posibilă datorită slăbiciunilor critografice pe care Enigma le avea care în combinație cu greșelile de operare, defectele procedurale sau capturarea unor caiete cu coduri ale naziștilor au decis într-o anumită măsură soarta războiului. Un alt ajutor în vederea ,,învingerii" mașinăriei Enigma a fost dat de către englezul Alan Turing care în anul 1940 a inventat o mașină numită Bomba, mașină ce avea ca scop ușurarea eforturilor depuse de armata britanică. [7]
În opinia multora, criptografia modernă a început cu Claude Elwood Shannon, un matematician american și un cunoscut în domeniul criptografiei, ce a contribuit în ceea ce privește criptanaliza în timpul celui de-al doilea război mondial. Claude Elwood Shannon este cunoscut și ca părinte al domeniului teoriei informației, el încadrând criptografia în era criptografiei matematice. Alte opinii spun că începutul criptografiei moderne este legat de codul lui Horst Feistel sau de începuturile criptografiei cu cheie publică ce i se datorează lui Diffie-Hellman-Merkel. Nu putem însă stabili cu adevărat unde a început era criptografiei moderne dar putem avea certitudinea că toate aceste etape prin care criptografia a trecut încă din antichitate și până în ziua de azi au contribuit la modelarea criptografiei și a criptanalizei în științele ce ne sunt prezentate astăzi. [8]

Fig. 3 Mașina Enigma
Sursa: https://historia.ro/sectiune/general/enigma-povestea-secretelor-germaniei-naziste-585325.html

1.3. Importanța protejării informațiilor în mediul digital

Protejarea informațiilor din mediul public digital a ajuns să fie de o importanță deosebită atât pentru indivizi cât și pentru instituțiile statului sau pentru marile companii. Datorită creșterii gradului de digitalizare s-a ajuns la o cantitate din ce în ce mai mare de informații sensibile ce trebuiesc a fi stocate și transmise în siguranță în mediul online. Odată cu creșterea cantității de informație din mediul digital a crescut și numărul de atacuri cibernetice ce au ca scop accesarea neautorizată a informației, furtul de date sau alterarea informației. Putem observa cum tehnologia avansează de la o zi la alta și sunt create tehnici din ce în ce mai avansate de protecție a datelor. În paralel cu acestea se dezvoltă și partea rău intenționată a mediului public ducând astfel la o luptă continuă pentru protejarea informațiilor din mediul public digital. Consecințele care apar în cazul în care datele nu sunt protejate într-un mod corespunzător sunt atât de tip financiar cât și de tip moral. Atacurile ce vizează informațiile din mediul digital au deseori consecințe de natură materială dar și unele de natură morală. Astfel, securitatea informațiilor este o componentă esențială în ceea ce privește stocarea și transmiterea acestora în mediul public digital. Protejarea informațiilor se realizează prin implementarea unor măsuri ce implică o serie de parole puternice, o tehnică de criptare a informației, o serie de aplicații și firewall-uri dar și o altă componentă la fel de importantă: realizarea de backup-uri ale informațiilor. Prin intermediul prioritizării protecției datelor atât indivizii cât și organizațiile își pot asigura siguranța și integritatea datelor și pot păstra totodată un grad crescut al încrederii în ceea ce privește mediul public digital.

1.4. Tehnici de criptare și decriptare a informației

Pentru a putea prezenta și a descrie diverse tehnici de criptare trebuie să începem prin a-i clasifica în funcție de diferite criterii. Cel mai important criteriu de clasificare este simetria algoritmului cu care se realizează criptarea. După acest criteriu, algoritmii se împart în două categorii:

- Algoritmi de criptare simetrici (Fig. 4);
- Algoritmi de criptare asimetrici (Fig. 5).

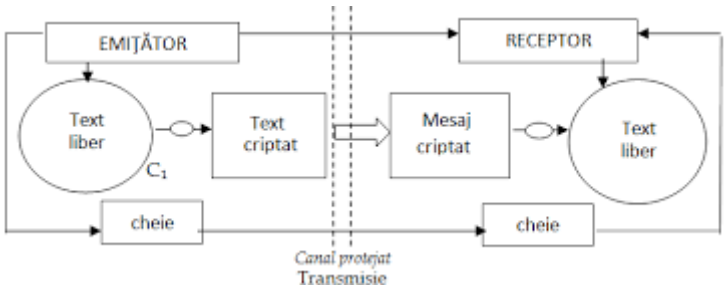


Fig. 4 Algoritm de criptare simetric
Sursa: https://www.researchgate.net/figure/Criptarea-si-decriptarea-unui-text-liber-cu-algoritm-asimetric-7-C-1-criptare-cu-cheie_fig3_318877856

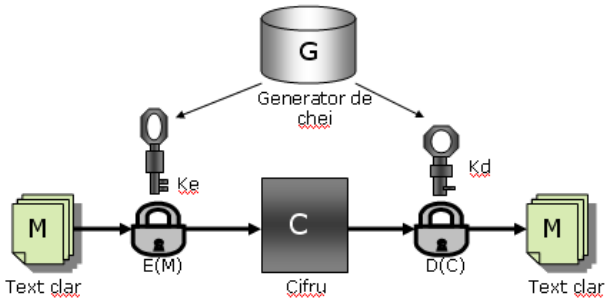


Fig. 5 Algoritm de criptare asimetric
Sursa: https://pclaptop.ro/despre-criptarea-asimetrica/

Prima categorie, cea a algoritmilor de criptare simetrici este caracterizată de folosirea aceleași chei, fie ea secretă sau privată, în procesul de criptare și decriptare a informației. Astfel, cei mai importanți algoritmi ce fac parte din această categorie sunt:

- DES – Data Encryption Standard
- TDES – Triple Data Encryption Standard
- AES – Advanced Encryption Standard

Cea de-a doua categorie, cea a algoritmilor de criptare asimetrici utilizează chei de criptare publice ce pot fi transmise cu ajutorul internetului (acestea sunt denumite PKC- Public Key Cryptography). Pentru criptarea unor secvențe scurte cum ar fi parole, certificate digitale, chei, identificatori etc. se utilizează algoritmi cu cheie publică ca de exemplu algoritmii RSA (Rivest-Shamir-Adleman și ElGamal.

În funcție de informația ce trebuie protejată, de nivelul de securitate pe care aceasta îl necesită, de nivelul de risc acceptat și de costurile pe care acest proces le implică (costuri ce pot fi financiare, de timp, de resurse umane etc.) se va alege algoritmul de criptare potrivit pentru protejarea informației.

Un alt mod de a clasifica algoritmii se bazează pe tipul de date prelucrate de acesta. Datele pot fi:

- Secvențe de biți;
- Valori zecimale întregi;
- Numere întregi dintr-un inel matematic;
- Câmp algebric infinit. [9]

Criptarea DES a apărut în anii 1970 în Statele Unite ale Americii. Algoritmul a fost creat de NBS (National Bureau of Standards- Biroul Național de Standardizare) în parteneriat cu NSA (National Security Agency- Agenția Națională de Securitate). Tehnica DES de criptare este una dintre cele mai folosite tehnici de criptare la nivel Mondial. Data Encryption Standard a fost creat pentru a asigura standardul protecției datelor comerciale neclasificate. Șase ani mai târziu, în 1976, compania IBM a implementat algoritmul DES sub denumirea de Lucifer. Acest algoritm se bazează pe blocuri de 64 de biți de date aplicând un număr de doar două operații asupra intrării. Cele două operații ce se aplică asupra intrării sunt deplasarea și substitția de biți. Astfel, algoritmul folosește o reprezentare binară a caracterelor utilizate în reprezentarea informației ce urmează a fi criptată. Procesul de codificare al datelor este controlat de cheia de criptare, cheie care este necesară pentru decriptarea datelor. Cheia inițială de criptare generează în timpul celor 16 runde de codificare 16 subchei de criptare (în fig. 6 poate fi observant algoritmul cu cele 16 runde de codificare și cele 16 subchei). În cazul acestui tip de criptare întâlnim principiul diversiunii ce presupune realizarea unei permutări inițiale și finale a informațiilor din fiecare bloc. Algoritmul DES a fost folosit în aplicații guvernamentale și în cele militare până la înlocuirea lui în anul 1999 de Standardul de criptare avansată AES (Advanced Encrptyon Standard). În cazul operațiunilor bancare și a datelor personale conținute de CIP-urile din pașapoarte a fost utilizată o versiune avansată a algoritmului DES și anume algoritmul TDES.

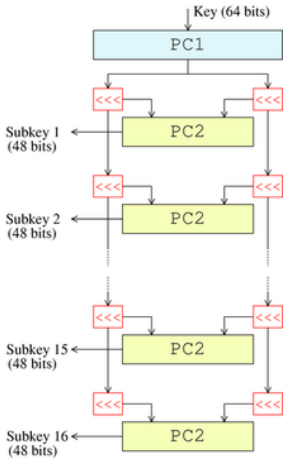


Fig. 6 Algoritm DES
Sursa: https://www.securitatea-informatiilor.ro/solutii-de-securitate-informatica/algoritmul-de-criptografie-des/

Triple Data Encryption Standard sau TDES așa cum este prescurtat are la bază tot algoritmul DES care este aplicat de trei ori rezultând un process ce conține 48 de runde de criptare ce sunt realizate de această data cu chei de criptare de 128 de biți. Prin aplicarea unui algoritm de tip TDES obținem o protecție mai bună a datelor în comparație cu algoritmul DES, comparabilă în cee ace privește robustețea cu algoritmul AES.

Advanced Encryption Standard este la acest moment cel mai eficient algoritm de criptare dintre cele trei. Acesta folosește un algoritm simetric de criptare ce se bazează pe chei de criptare secrete ce pot avea dimensiunea de 128, 192 sau 256 de biți. Operațiile sunt realizate pe blocuri de octeți și sunt catalogate ca fiind simple din punct de vedere al complexității de calcul. Ele includ o combinație de permutări, adunări, substituții și produse în câmpuri Galois. [9] Câmpurile Galois sunt câmpuri numerice finite ce au operații interne de adunare și multiplicare. Utilizări ale algoritmului AES sunt întâlnite în metoda de securizare a rețelelor wireless WPA (Wifi Protected Access), pentru criptarea traficului de date din rețele de tip VPN (Virtual Private Network) dar și în protocoalele de tip TLS (Transport Layer Security) și IPsec (Internet Protocol Security).

Un alt algoritm ce utilizează o cheie publică de criptare este algoritmul RSA (Rivest-Shamir-Adleman). El poate fi folosit de altfel și pentru semnătura digitală. Denumirea algoritmului vine de la numele inventatorilor săi și anume: Ron Rivest, Adi Shamir și Len Adleman. RSA este asemeni algoritmilor prezentați anterior, un algoritm de criptare pe blocuri. Ambele texte (atât textul clar cât și cel cifrat) sunt numere cuprinse între 0 și n-1, cu mențiunea că n este ales. Dacă mesajul are o dimensiune ce depășește valoarea de $\log n$ acesta va fi împărțit în mai multe segmente de lungimi corespunzătoare. Segmentele respective sunt numite blocuri și sunt cifrate pe rând, una câte una. O altă caracteristică a acestui algoritm este funcționalitatea acestuia bazată pe o pereche de chei (o cheie publică, accesibilă oricui și o cheie secretă care este cunoscută doar de deținătorul ei) ce sunt matematic legate între ele. [10] Algoritmul RSA este recomandat pentru criptarea secvențelor scurte de date deoarece acest algoritm necesită o capacitate mare de calcul.

1.5. Metodele de protejare a informației în mediul public digital

Potrivit dr. Ioan Gogota, în articolul său intitulat „Protecția datelor personale și mediul online”, având în vedere noile provocări cu care se confruntă sectoarele IT&C, precum amenințările cibernetice care reprezintă o amenințare semnificativă pentru securitatea națională, precum și capacitatea de a preveni atacurile cibernetice care sunt extrem de dificil de identificat (exploatând vulnerabilitățile umane din spațiul virtual), este foarte important să existe politici și proceduri clare de securitate, precum și un management eficient al sistemelor informatice și de tehnologii. În fiecare zi, atât acasă, cât și la locul de muncă, suntem vulnerabili la amenințări din spațiul virtual, care sunt cauzate de infrastructurile cibernetice, care includ conținutul informațional procesat, stocat sau transmis, precum și acțiunile realizate de utilizatori. Aceste

amenințări sunt esențiale pentru viața personală și profesională, iar securitatea mediului virtual este rareori luată în considerare. Utilizatorii de Internet, care de obicei nu sunt conștienți de pericole, iau măsuri care cred că ar trebui să le ofere o protecție adecvată. În cazul în care acțiuni ostile pot afecta funcționarea sistemelor informatice și datele vehiculate în mediul virtual, se impun măsuri de securitate. Aceste măsuri sunt necesare deoarece mediul virtual are din ce în ce mai multe legături cu spațiul fizic, inclusiv formulare online care conțin date personale, informații financiare și contractuale despre angajați și baze de date. În timp, accesul terților la documente confidențiale poate duce la pierderi financiare semnificative. [11]
Într-un raport recent realizat de Kaspersky, s-a descoperit că peste jumătate dintre utilizatorii de Internet (56%) cred că confidențialitatea completă în lumea digitală contemporană este imposibilă. Este ușor de înțeles motivul acestei convingeri. Internetul a devenit foarte legat de tot ceea ce facem, de la cumpărături și vizionare de filme până la următorul pas în carieră, socializare și bancare, deoarece nouă din zece (89%) persoane intră online de mai multe ori pe zi. Chiar tipul de conținut pe care îl vedem în acțiunile noastre online se reflectă, cum ar fi reclamele care li se adresează, făcându-i să se simtă ca și cum ar fi intrat în spațiul lor privat. În consecință, este internetul o zonă de pace sau una de conflict?
Cercetările Kaspersky au arătat că aproximativ 33% dintre oameni nu știu cum își pot proteja complet confidențialitatea online. În timp ce unii oameni cred că nu au suficientă putere pentru a se opune încălcării vieții lor private, alții cred că nu au suficientă putere. Îngrijorător, mai mult de un utilizator din zece (13%) nu mai este interesat de modul în care ar putea îmbunătăți confidențialitatea datelor sale. Deși percepțiile despre viața privată sunt diferite de la o persoană la alta, există repercusiuni reale atunci când informațiile personale sunt folosite în mod abuziv sau ajung pe mâini greșite. În ciuda acestui fapt, 18% dintre oameni ar renunța cu ușurință la confidențialitate și ar împărtăși informațiile personale în schimbul unui lucru gratuit. Partajarea pe rețelele de socializare poate fi, de asemenea, o spirală descendentă, deoarece mulți oameni neglijează informațiile personale pe internet în încercarea de a obține câștiguri imediate și „like-uri" pe rețelele de socializare, ceea ce poate avea repercusiuni catastrofale pe termen lung. Într-un caz făcut public în mass-media, presupusul lider al grupului care a jefuit-o pe Kim Kardashian la Paris în 2016 susține că el și asociații săi au aflat despre călătoria ei de pe rețelele sociale înainte de furt, astfel încât au putut să evalueze valoarea bijuteriilor pe care aceasta le deținea. Deși acest lucru poate părea un exemplu extrem, este tot mai obișnuit ca angajatorii și potențialii angajatori să verifice pe LinkedIn, Instagram, Facebook și Twitter dacă angajații și candidații au o reputație pozitivă și dacă angajații nu dau o impresie proastă despre companie. [12]

Reprezentanții Kaspersky[4] oferă următoarele sfaturi pentru a preveni utilizarea necorespunzătoare a datelor personale:

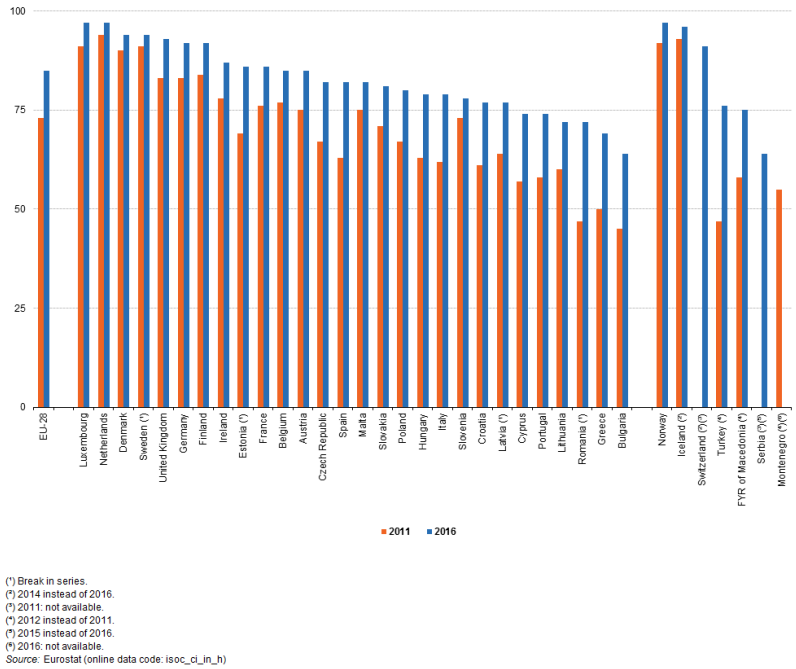
- Gândiți-vă bine înainte de a posta pe rețelele sociale. Ar putea exista consecințe grave dacă dezvăluiți anumite informații sau opinii personale? Poate fi folosit conținutul postat împotriva dumneavoastră în prezent sau în viitor?
- Nu împărtășiți parolele contului dumneavoastră online cu prietenii sau familia dumneavoastră. Deși împărtășirea conturilor cu cei dragi poate părea o idee bună sau comodă, există o probabilitate mai mare ca atacatorii să găsească parolele. În cazul în care una dintre aceste relații personale se deteriorează, păstrați-le secrete pentru a vă proteja confidențialitatea.
- Pentru a reduce expunerea, protejați-vă datele personale pe internet, împărtășind sau permițând terților acces la datele dumneavoastră doar dacă este absolut necesar.
- Folosirea unor programe de securitate și utilizarea a mai multe parole diferite, este un exemplu care poate reduce riscurile și proteja datele personale în mediul online.

1.6. Informațiile din mediul public și încrederea populației

Viața de zi cu zi a oamenilor este influențată de tehnologia informației și comunicațiilor în multe moduri, atât la locul de muncă, cât și acasă, un exemplu fiind acela când comunică sau

[4] Kaspersky este o companie software ce produce programe de securitate pentru companii și utilizatorii mediului digital.

cumpără lucruri online. Politicile Uniunii Europene acoperă o gamă largă de domenii, ce variază de la comerțul electronic până la eforturi de a proteja viața privată a persoanelor și ajungând chiar la reglementarea unor sectoare întregi. În acest subcapitol am decis să analizez un raport al Eurostat ce conține diferite statistici în ceea ce privește societatea și economia digitală din țările membre ale Uniunii Europene.
În ceea ce privește accesul și costurile, tehnologiile informației și comunicațiilor au devenit mai accesibile pentru o populație largă. În 2007, majoritatea gospodăriilor din UE[5] aveau acces la internet, pragul de 50% fiind depășit (reprezentând jumătate din numărul total al gospodăriilor din UE). În continuare, procentul a crescut, depășind trei sferturi în 2012 și patru cincimi în 2014. În UE, proporția gospodăriilor cu acces la internet a crescut cu 2 puncte procentuale comparativ cu 2015, ajungând la 85 la sută. Acest procent a crescut cu 30 de puncte procentuale mai mult decât cel din 2007. În figura 7 se poate observa accesul la internet al gospodăriilor, în anul 2011 și 2016 în toate statele membre ale Uniunii Europene.



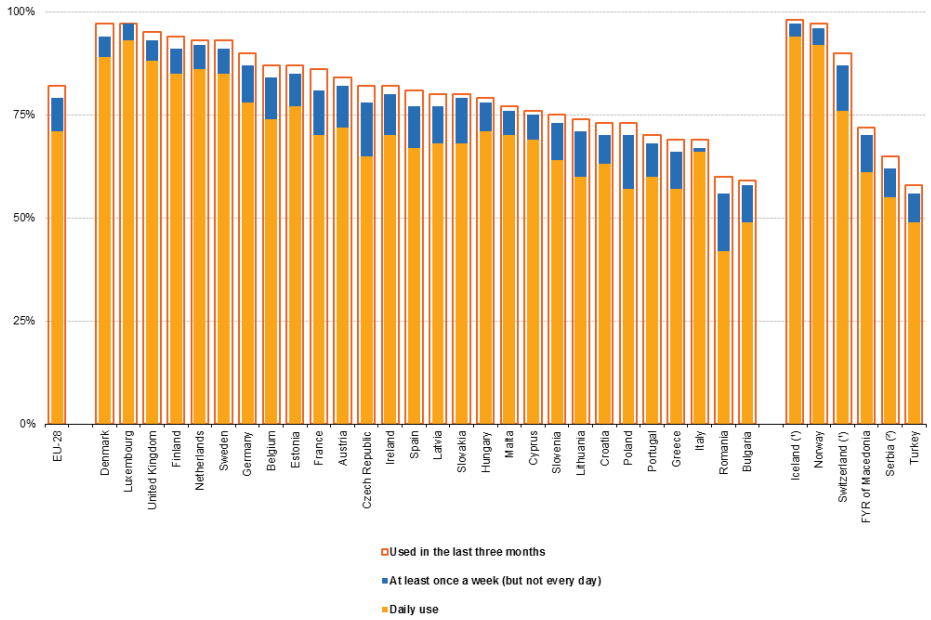
(*) Break in series.
(*) 2014 instead of 2016.
(*) 2011: not available.
(*) 2012 instead of 2011.
(*) 2015 instead of 2016.
(*) 2016: not available.
Source: Eurostat (online data code: isoc_ci_in_h)

Fig. 7 Accesul la internet al gospodăriilor, 2011 și 2016
Sursa: Eurostat

Peste 82% din toate persoanele din UE cu vârste cuprinse între 16 și 74 de ani au utilizat internetul la începutul anului 2016, cel puțin o dată în ultimele trei luni anterioare cercetării. În Danemarca, Luxemburg, Regatul Unit, Finlanda, Țările de Jos, Suedia și Germania, cel puțin 90% dintre oameni au utilizat internetul. În comparație, puțin peste două treimi din toate persoanele cu vârsta cuprinsă între 16 și 74 de ani au folosit internetul. Acest lucru a fost observat în Portugalia (70%), Grecia (69%) și Italia (69%). În România, acest procent a scăzut la 60% și în Bulgaria la 59%.

În 2016, 14% dintre cetățenii UE nu au folosit niciodată internetul, o scădere de la 37% în 2007 și 24% în 2011. Peste două treimi (71%) din persoanele din UE au folosit internetul zilnic în 2016, conform figurii 8. De asemenea, 8% au folosit internetul cel puțin o dată pe săptămână, dar nu zilnic. Astfel, 79% dintre oameni foloseau internetul frecvent, cel puțin o dată pe săptămână. În UE, rata utilizatorilor de internet zilnici (cei care au utilizat internetul în ultimele trei luni) a fost în medie de 87 la sută. Rata a fluctuat între statele membre ale UE, de la 71 la sută în România, 78 la sută în Polonia și 79 la sută în Republica Cehă, la 92 la sută în Danemarca, 93 la sută în Țările de Jos și Regatul Unit, 95 la sută în Luxemburg și 96 la sută în Italia. Conform datelor obținute, un procent de 95% din populația Norvegiei și a Islandei folosea internetul zilnic. Aceste date sunt reprezentate sub forma unui grafic în figura 8.

[5] UE- Uniunea Europeană

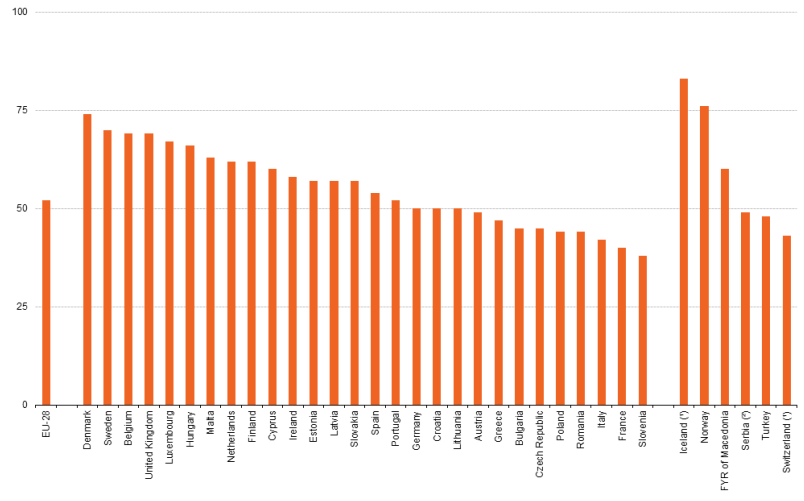


(*) 2014.
(*) 2015.
Source: Eurostat (online data codes: isoc_ci_ifp_iu and isoc_ci_ifp_fu)

Fig. 8 Frecvența utilizării internetului, 2016 (% din persoanele cu vârste cuprinse între 16 și 74 de ani)
Sursa: Eurostat

Participarea la rețelele sociale a fost una dintre cele mai frecvente activități online din UE în 2016. Peste cincizeci și două la sută dintre persoanele cu vârste cuprinse între 16 și 74 de ani au utilizat internetul pentru a participa la rețelele sociale, utilizând site-uri precum Facebook sau Twitter.

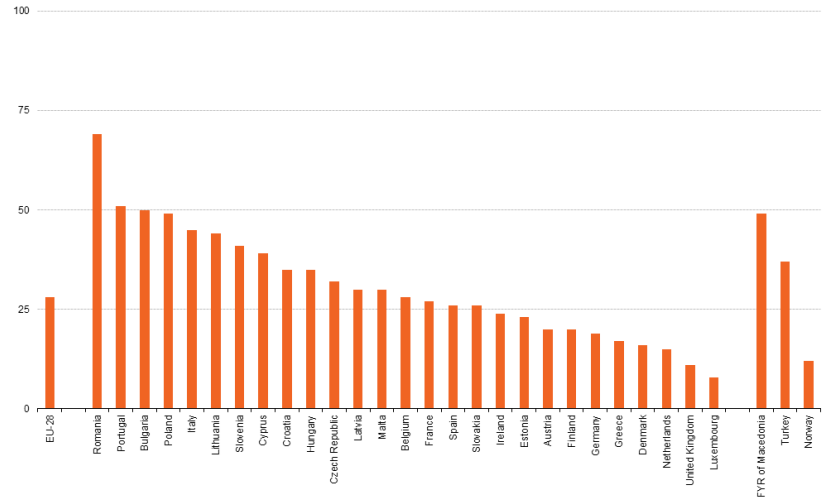
Aproximativ două treimi (66–70 %) din oamenii din Ungaria, Luxemburg, Regatul Unit, Belgia și Suedia au utilizat site-uri de rețele sociale. Această rată a fost de 74 la sută în Danemarca, 76 la sută în Norvegia și 83 la sută în Islanda (în 2014). În schimb, două state membre ale UE, Franța (40 %) și Slovenia (38 %) au raportat că cel mult 4 din 10 oameni au folosit astfel de site-uri. În figura 9 se poate vedea procentul persoanelor ce au utilizat internetul pentru a accesa rețele sociale în anul 2016.



(*) 2014.
(*) 2015.
Source: Eurostat (online data code: isoc_bde15cua)

Fig. 9 Persoane care au utilizat internetul pentru a participa la rețelele sociale, 2016
(% din persoanele cu vârste cuprinse între 16 și 74 de ani)
Sursa: Eurostat

În 2016, au existat diferențe între statele membre ale UE în ceea ce privește modul în care utilizatorii de internet au ales să își gestioneze accesul la informațiile cu caracter personal. În UE, peste 28% din utilizatorii de internet nu au furnizat informații personale. Acest număr variază de la doar 8% în Luxemburg la cel puțin 50% în Bulgaria, Portugalia și România (a se vedea figura 10).



Note: Sweden: not available.
Source: Eurostat (online data code: isoc_cisci_prv)

Fig. 10 Procentul persoanelor care nu au furnizat informații cu caracter personal pe internet, 2016 (% din persoanele care au utilizat internetul pe parcursul ultimului an)
Sursa: Eurostat

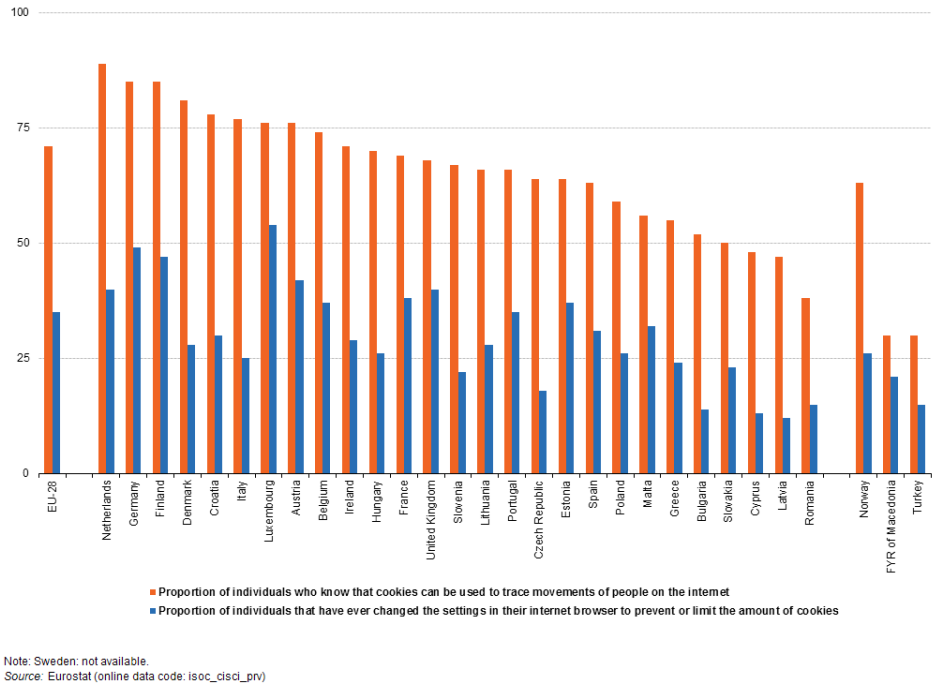
Astfel, peste 70 % din utilizatorii de internet din UE-28 au furnizat câteva tipuri de informații personale pe internet, iar mulți dintre aceștia au luat diferite măsuri pentru a controla accesul lor la aceste informații personale pe internet. Aproape jumătate dintre toți utilizatorii de internet (46 la sută) au refuzat să permită utilizarea informațiilor personale în scopuri publicitare, iar două cincimi (40 la sută) au restricționat accesul la profilurile sau conținutul lor pe site-urile de rețele sociale. În plus, peste o treime (37 %) din utilizatorii de internet au citit declarațiile privind politica de confidențialitate înainte de a oferi informații personale, în timp ce mai puțin de o treime (31 %) au restricționat accesul la locația geografică.

În 2016, 71 la sută dintre persoanele cu vârste cuprinse între 16 și 74 de ani din UE au fost conștiente de faptul că modulele cookie pot fi utilizate pentru an urmări activitatea utilizatorilor pe internet în ultimele 12 luni. Aproximativ 74 la sută dintre utilizatorii tineri (cu vârste cuprinse între 16 și 24 de ani) și 64 la sută dintre utilizatorii mai în vârstă (cu vârste cuprinse între 55 și 74 de ani) au fost conștienți de acest aspect. Peste o treime (35 %) dintre utilizatorii cu vârste cuprinse între 16 și 74 de ani au declarat că au modificat configurațiile browserului[6] lor internet pentru a opri sau limita utilizarea modulelor cookie[7] (a se vedea figura 11).

Utilizatorii de internet din Țările de Jos (89 %), Germania și Finlanda (ambele cu 85 %) au fost cei mai conștienți de utilizarea modulelor cookie pentru an urmări activitatea lor online. În plus, nivelul de conștientizare a fost unul ridicat în Danemarca (81 %), Croația (78 %), Italia (77 %), Luxemburg și Austria (ambele cu 76%). În schimb, mai puțin de jumătate din utilizatorii de internet au fost conștienți de acest fapt în România (38 %), Letonia (47 %) și Cipru (48 %), iar în Turcia și Macedonia (30 %). Luxemburg a fost singurul stat membru al Uniunii Europene în care peste jumătate dintre utilizatorii de internet au modificat setările browserului pentru a opri sau limita utilizarea modulelor cookie. În schimb, mai puțin de o cincime dintre utilizatorii de

[6] Browser- program care permite utilizatorilor să afișeze text, grafică, video, muzică și alte informații situate pe o pagină din World Wide Web.
[7] Module cookie- sunt mici fișiere de text pe care un site le plasează pe calculatorul sau pe dispozitivul mobil atunci când site-ul este accesat.

internet au luat astfel de acțiuni în Republica Cehă, România, Bulgaria, Cipru și Letonia, precum și în Turcia.



Note: Sweden: not available.
Source: Eurostat (online data code: isoc_cisci_prv)

Fig. 11 Utilizarea modulelor cookie și a setărilor browserului, 2016 (% din persoanele care au utilizat internetul pe parcursul ultimului an)
Sursa: Eurostat

Capitolul 2. Vulnerabilități ale sistemelor informatice în fața atacurilor cibernetice

2.1. Ce este un atac cibernetic?

Sintagma „atac cibernetic" a devenit din ce în ce mai frecventă în societatea zilelor noastre, societate ce se află într-o continuă transformare ce are la bază nevoia de interconectare prin intermediul internetului. Orice activitate rău intenționată care vizează sisteme informatice, rețele sau dispozitive cu intenția de a fura sau de a distruge informații, de a interfera cu serviciile sau de a provoca daune în alt mod este denumită „atac cibernetic". Atacurile cibernetice, care pot avea multe forme diferite, reprezintă o amenințare gravă pentru oameni, companii și guverne deopotrivă. [13] Atacurile cibernetice sunt încercări intenționate de a evita securitatea dispozitivelor, rețelelor sau sistemelor digitale pentru a fura, a corupe sau a modifica date sensibile, a perturba afacerile sau pentru a obține acces neautorizat la datele și informațiile pe care acestea le stochează și le tansmit. Frecvența și complexitatea atacurilor cibernetice a crescut în ultimii ani ca urmare a dependenței tot mai mari a oamenilor de tehnologie și internet, reprezentând o amenințare serioasă pentru oameni, companii și guverne din întreaga lume. În zilele noastre, majoritatea interacțiunilor economice, comerciale, culturale, sociale și guvernamentale ale națiunii se desfășoară în spațiul cibernetic. Aceasta implică interacțiuni între indivizi, organizații neguvernamentale, guverne și instituții guvernamentale. Multe întreprinderi private și instituții guvernamentale din întreaga lume se confruntă în prezent cu problema atacurilor cibernetice și cu riscul prezentat de tehnologiile de comunicații fără fir. Societatea modernă se bazează în mare măsură pe tehnologia electronică, așa că protejarea acestor date de atacurile cibernetice este o problemă dificilă. [14] Pentru a înțelege amploarea și numărul atacurilor cibernetice ce au avut loc în ultimii ani, compania de suport IT AAG a centralizat următoarele date statistice ce evidențiază creșterea numărului de infracțiuni cibernetice. Potrivit datelor statistice, criminalitatea cibernetică a crescut cu 358% în anul 2020 față de anul precedent ca urmare a transferului muncii de la birou în mediul online, schimbare ce a fost impusă de pandemia de COVID-19. În următorul an, 2021, a fost înregistrată o creștere globală cu 125% a numărului de atacuri cibernetice. Aceeași statistică scoate în evidență și următoarele date:

- Aproape 1 miliard de email-uri au fost expuse atacurilor cibernetice într-un singur an, astfel fiind afectați 1 din 5 utilizatori de internet;
- În medie, scurgerile de date ale companiilor au produs daune de 4.35 milioane de dolari în anul 2022;
- În prima jumătate a anului 2022 au fost înregistrate peste 236 de milioane de atacuri cibernetice la nivel global;

Un procent de 39% din companiile ce își desfășoară activitatea în Marea Britanie au raportat că au suferit atacuri cibernetice asupra datelor. [15]

2.2. Istoria atacurilor cibernetice

Criminalitatea cibernetică a devenit o industrie de 1,5 trilioane de dolari (USD) cu un întreg ecosistem de afaceri care funcționează ca afaceri legitime în ultimii zece ani. În ciuda faptului că industria criminalității cibernetice a crescut în ultimii zece ani, criminalitatea cibernetică nu este o amenințare nouă. De fapt, datează de secole și nu doar de câteva decenii.

Din punct de vedere tehnic, primul atac cibernetic a avut loc în Franța în 1834, cu mult înainte ca internetul să fie creat. Atacatorii au obținut acces la sistemul telegrafic francez și au furat informații referitoare la piețele financiare. De atunci, criminalitatea cibernetică a crescut substanțial și se caracterizează printr-o evoluție intrigantă a strategiilor, tacticilor și procedurilor care sunt toate folosite în scopuri dăunătoare. Cu toate acestea, abia la mijlocul secolului al XX-lea a început să descopere criminalitatea cibernetică. Infractorii cibernetici au fost impulsionați de revoluția digitală să devină primii utilizatori ai tehnologiei. Și-au folosit previziunea și ingeniozitatea pentru a crea strategii noi și viclene de a fura bani și date de la persoane și companii.

Istoria modernă a criminalității cibernetice începe în anul 1962, an în care Allen Scherr lansează un atac cibernetic asupra rețelei de calculatoare a MIT (Massachusetts Institute Of Tehnology), furând astfel parole din baza lor de date cu ajutorul cartelei perforate (fig. 12). [16] Cardurile de hârtie cu găuri perforate pentru a reprezenta datele și instrucțiunile computerului sunt cunoscute sub denumirea de cartele perforate (sau în limba engleză „punched cards”), carduri Hollerith sau carduri IBM. Erau o modalitate obișnuită pentru oameni de a introduce date în computerele timpurii. Cartelele au fost introduse într-un cititor de carduri care a fost atașat la un computer, care transpunea ordinea găurilor în date digitale. [17]

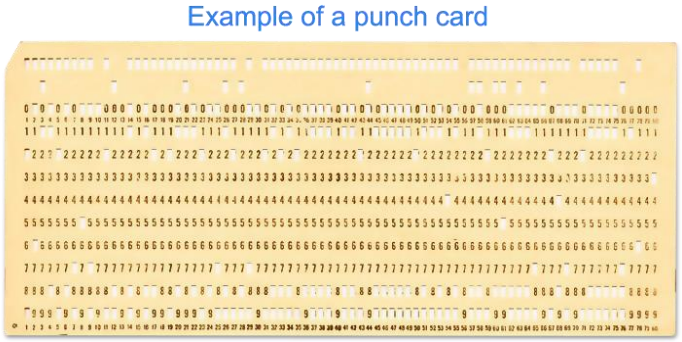


Fig. 12 Cartelă perforată
Sursa: https://www.computerhope.com/jargon/p/punccard.htm

Bob Thomas de la BBN Technologies a inventat primul virus informatic ca proiect de cercetare. Programul cu auto-replicare, cunoscut sub numele de Creeper Virus, a fost descoperit pe ARPANET[8] în 1971 și a anticipat potențialul ca virușii de mai târziu să dăuneze grav sistemelor informatice. Deși virusul Creeper a deteriorat sistemul, acesta nu a furat sau corupt datele așa cum o fac virușii moderni, ci doar a afișat un mesaj pentru a demonstra transmiterea și răspândirea informațiilor de la un calculator la altul. În anul 1981, după ce a pătruns cu succes

[8] ARPANET- acronim pentru Advanced Research Projects Agency Network

în sistemele interne ale AT&T[9] și a schimbat ceasurile computerelor lor, făcând ravagii, Ian Murphy a devenit prima persoană care a fost găsită vreodată vinovată de comiterea unei infracțiuni cibernetice. Șapte ani mai târziu, în anul 1988 a avut loc primul atac cibernetic semnificativ asupra internetului. Înainte de lansarea World Wide Web, Robert Morris un absolvent al Univeristății Cornell din New York, a lansat un atac prin intermediul „Viermelui Morris" ce a reușit să infecteze computerele de la universități de prestigiu precum Stanford, Princeton, John Hopkins, UC Berkeley dar și a computerelor NASA[10]. Acest vierme cibernetic a început să se răspândească incredibil de rapid și să afecteze computerele. Mai târziu în acea seară, un student îngrijorat de la Universitatea Berkeley din California a trimis un e-mail în care spunea: „Suntem în prezent atacați". Aproximativ 6.000 din cele 60.000 de computere conectate la internet la acea vreme au fost atacate în 24 de ore. Spre deosebire de viruși, viermii de computer pot exista și se pot răspândi singuri, fără ajutorul unui program gazdă. Viermele s-a limitat la compueterele care rulau o anumită versiune a sistemului de operare Unix, dar s-a răspândit rapid datorită numeroaselor sale căi de atac. De exemplu, a folosit un defect în programul „deget" (în limba engleză „Finger") utilizat pentru recunoașterea utilizatorilor rețelei, împreună cu o modalitate alternativă de utilizare a sistemului de e-mail[11] folosit pe internet. Atacul a fost unul puternic, în ciuda faptului că nu a corupt sau șters fișiere din sistemele infectate. Operațiunile militare și academice importante au fost încetinite în timpul atacului unele dintre acestea fiind chiar oprite. În unele cazuri pentru a putea transmite un e-mail au fost necesare mai multe zile. Pentru a înțelege cum acest vierme funcționează și cum poate fi oprit, specialiștii au lucrat neîncetat timp de mai multe zile. Unele din companiile și organizațiile afectate au recurs la ștergerea întregului lor sistem, în timp ce altele s-au rezumat doar la a deconecta temporar computerele de la rețeaua de internet. Daunele produse de acest atac cibernetic au fost cu greu calculate dar estimările au variat între suma de 100.000 de dolari și câteva milioane de dolari. Agenția FBI[12] a lansat o investigație pentru a rezolva cazul și l-a audiat pe Robert Morris împreună cu complicii săi, în computerele acestora fiind găsite dovezi incriminatorii. În următorul an, instanța de judecată l-a găsit pe Morris vinovat de încălcarea legii și l-a condamnat pe acesta la 400 de ore de muncă în folosul comunității și plata unei amenzi pentru daunele provocate, acesta scăpând totuși de pedeapsa cu închisoarea. Acest incident a inspirat o nouă generație de atacatori cibernetici și a adus în atenția publicului vremii importanța pe care sistemele informatice le au și consecințele neprotejării acestora. [18]

Odată cu dezvoltarea internetului și răspândirea pe scară largă a acestuia la nivel mondial, anii '90 au dat naștere unora dintre cele mai bune tehnologii de comunicare cunoscute de omenire până la acel moment. Aceste evoluții au venit la pachet și cu un cost și anume criminalitatea cibernetică a ajuns la cote nemaiîntâlnite pentru acele vremuri, atât din punct de vedere al numărului de atacuri cât și al complexității acestora. Infractorii cibernetici au profitat de faptul că la începutul noilor tehnologii accentul era pus pe creerea și dezvoltarea unor noi aplicații, siguranța nefiind un factor important la acel moment. Securitatea cibernetică nu era un termen de referință al acelei perioade așa că a fost ignorată în detrimentul inovării pe piața comunicării și a afacerilor. În tot acest timp, în paralel cu acestea, se dezvolta o economie și o comunitate mai puțin binevoitoare ce avea să câștige din ce în ce mai mulți adepți în următoarea perioadă de timp. Creșterea ratei criminalității cibernetice a indicat că atacatorii profitau de noi șanse și inventau modalități inovatoare de a pătrunde în rețele fără autorizație și de a modifica datele online. În anul 1995 are loc primul atac cibernetic înregistrat asupra unei bănci. Responsabil pentru acesta a fost Vladimir Levin (fig. 13), un cetățean rus ce și-a câștigat notorietatea prin atacarea sistemului informatic al Citibank, una dintre cele mai mari bănci ale vremii. Acesta a accesat fraudulos sistemul informatic al băncii și a realizat numeroase tranzacții către o multitudine de conturi din diverse colțuri ale lumii. Prejudiciul adus băncii Citibank a fost de aproximativ 10 milioane de dolari americani. În același an, trei dintre complicii acestuia au fost arestați în timp ce încercau să retragă banii transferați la bancomate din Israel, Olanda sau Statele Unite ale Americii. Aceste arestări au dus și la localizarea lui Levin, ce a fost arestat la

[9] AT&T- cea mai mare companie de telecomunicații din Statele Unite ale Americii
[10] NASA- acronim pentru National Aeronautics and Space Administration – Administrația Națională Aeronautică și Spațială
[11] E-mail – electronic mail (în traducere din limba engleză: poștă electronică)
[12] FBI- Federal Bureau of Investigation (în traducere din limba engleză: Biroul Federal de Investigații)

rândul său în martie 1995 pe aeroportul Stansted din Londra. Doi ani mai târziu, cererea de extrădare a fost aprobată iar Vladimir Levin a fost adus în fața justiției americane. Astfel, a fost realizată prima arestare a unui criminal cibernetic ce intrase în sistemul unei bănci și reușise să transfere banii în alte conturi. După această întâmplare, Citibank dar și restul băncilor mari de la acea vreme au decis să își sporească măsurile de securitate împotriva atacurilor cibernetice prin implementarea cardului de criptare dinamic[13]. [16]

Fig. 13 Vladimir Levin, atacatorul Citibank
Sursa: https://medium.com/@anglee19/vladimir-levin-hacks-citibank-910627591237

La finele anilor ’90, virușii informatici nu erau un subiect prea cunoscut în societatea americană, noțiunea fiind fie necunoscută fie vaf cunoscută de utilizatorii calculatoarelor de la acea vreme. Astfel, la sfârșitul lunii martie a anului 1999, are loc atacul ce urma să schimbe înțelegerea oamenilor asupra virușilor informatici. Virusul informatic este la bază un program ce se instalează singur, fără a cere acceptul utilizatorului, cu scopul de a provoca pagube atât în ceea ce privește sistemul de operare cât și componentele fizice ale calculatorului. [19] Atacul menționat mai sus a fost pus în aplicare de un programator american pe nume David Lee Smith ce a reușit să acceseze un cont al AOL[14] prin intermediul căruia a reușit să posteze într-unul din grupurile de știri de pe internet un fișier ce purta denumirea de ,,alt.sex”. Astfel, postarea le promitea tuturor utilizatorilor ce deschideau fișierul accesul la zeci de parole ce puteau fi folosite pentru a accesa site-uri cu conținut pentru adulți, site-uri la care în mod obișnuit accesul era realizat doar în urma unor plăți efectuate de utilizatori. Era un proces relativ simplu prin care victimele trebuiau doar să descarce fișierul respectiv și să îl deschidă în aplicația Microsoft Word, în urma deschiderii urmând ca virusul să fie dezlănțuit asupra calculatorului victimei. După ce virusul punea stăpânire pe aplicația Microsoft Word, următoarea victimă era sistemul de e-mail Microsoft Outlook. Acesta accesa contul utilizatorului și trimitea către primele 50 de persoane din lista acestuia un e-mail ce conținea documentul infectat ce era denumit în diverse moduri pentru a atrage noi victime în această capcană informatică. Virusul a fost denumit ,,Virusul Melissa” chiar de către David Lee Smith, creatorul acestuia. În urma răspândirii cu o viteză nemaivăzută pentru acele timpuri, virusul a reușit să infecteze mii de calculatoare. Chiar dacă acesta nu a fost creat cu intenția de a fura bani sau informații, a reușit să provoace pagube de peste 80 de milioane de dolari prin încetinirea sau blocarea a serverelor de e-mail din peste 300 de corporații și agenții guvernamentale din întreaga lume. Estimările făcute în urma atacului au concluzionat că aproximativ 1 milion de adrese de e-mail au fost afectate, fapt ce a dus la o scădere a traficului de internet, în unele zone până aproape de pragul opririi acestuia. Responsabilul pentru acest virus, David Lee Smith, a fost arestat în statul New Jersey din Statele Unite ale Americii pe 1 aprilie 1999 ca mai apoi acesta să pledeze vinovat în fața instanței de judecată în luna decembrie a aceluiași an. Sentința în cazul lui Smith a venit în mai 2002, fiind condamnat la 20 de luni de detenție într-o închisoare federală dar și la plata unei amenzi în valoare de 5000 de dolari americani. De asemenea, Smith a fost de accord să colaboreze cu autoritățile statale și federale pentru a-i ajuta în vederea creșterii siguranței în fața atacurilor cibernetice. [20]

[13] Tradus din limba engleză- Dynamic Encryption Card- este un principiu criptografic ce permite ambelor părți implicate într-o tranzacție să schimbe algorimtul de criptare în fiecare tranzacție.
[14] AOL- America Online

Prima decadă a mileniului trei a venit la pachet cu o multitudine de atacuri ce deveneau din ce în ce mai dezvoltate atât în ceea ce privește complexitatea metodelor folosite de atacatori cât și complexitatea rezolvărilor pe care aceste atacuri le presupuneau. Majoritatea atacurilor aveau de acum un nou actor ce avea să joace un rol deosebit de important în această bătălie cibernetică: statele lumii. Evoluția criminalității cibernetice presupunea utilizarea unor viruși și a unor viermi mai dezvoltați ca niciodată ce aveau să cauzeze pagube semnificative în economia globală digitală. Astfel, până la sfârșitul primei decade securitatea cibernetică a ajuns să fie o prioritate pentru utilizatorii de calculatoare și internet de pe întreg globul pământesc, cu precădere pentru guvernele statelor dar și pentru companiile mari din mediul privat. Primul atac notabil al secolului 21 a fost realizat de un adolescent în vârstă de 15 ani numit Michael Calse, cunoscut în mediul online sub pseudonimul de ,,Mafiaboy". Acesta a lansat o serie de atacuri de tip DDoS[15] (fig. 14) asupra unora dintre cele mai mari site-uri comerciale și de știri din lume. Printre acestea s-au numărat și firme precum Amazon, Yahoo, CNN sau eBay. Astfel, atacatorul a reușit să blocheze site-urile acestor companii pentru câteva ore rezultatul fiind reprezentat de pagube estimate la câteva milioane de dolari americani.

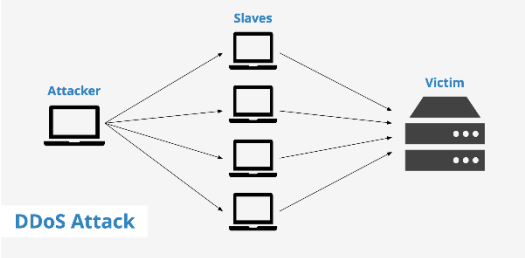


Fig. 14 Atac de tip DDoS
Sursa: https://www.keycdn.com/support/ddos-attack

Criminalitatea cibernetică a crescut dramatic în ultimii zece ani, crescând de la un sector mic și slab dezvoltat la o adevărată industrie. Atacatorii au creat noi programe și metode rău intenționate, care au crescut rata criminalității cibernetice și volumul zilnic de atacuri. Sectorul criminalității cibernetice nu a fost singurul sector ce a cunoscut o creștere imensă. Pe măsură ce percepția despre securitatea digitală a dispărut, companiile au început să angajeze mai mulți specialiști în securitate cibernetică pentru a combate pericolul atacurilor cibernetice. Acest lucru a dus la apariția unei discipline noi cunoscută sub numele de hacking etic, al cărei obiectiv principal este să găsească vulnerabilitățile înainte ca acestea să fie exploatate în mod rău intenționat. Această nouă disciplină a evoluat ca urmare a cerinței de protecție continuă a datelor. Organizațiile se află într-o poziție vulnerabilă când vine vorba de a se proteja împotriva diferitelor amenințări cibernetice din cauza evoluției și a sofisticacității crescânde a acestor amenințări și a modului în care sunt utilizate în atacuri.

Principalele atacuri care au produs cele mai multe pagube de-a lungul acestui deceniu au inclus introducerea unor noi viermi și viruși în cee ace privește sectorul informatic. În anul 2010 este creat ,,The Stuxnet worm" sau ,,viermele Stuxnet", cunoscut ca fiind prima ,,armă digitală" din istoria ciberneticii. Acest vierme a apărut prin colaborarea Agenției Naționale de Securitate a Statelor Unite ale Americii, a CIA[16] și a Centrului de Informații Israeliene. Viermele Stuxnet (Fig. 15) a fost conceput în primă fază pentru a ataca instalațiile nucleare ale Iranului, dar ulterior a evoluat și s-a răspândit în alte facilități industriale și producătoare de energie. Controlerele logice programabile (PLC-uri[17]) care sunt utilizate pentru a automatiza activitățile industriale au fost punctul central al atacului inițial al virusului Stuxnet. Când a fost găsit în

[15] DDoS- Distributed Denial of Service- tip de atac cibernetic prin care atacatorul ,,inundă" un server cu informații pentru a preveni utilizatorii să acceseze un anumit site
[16] CIA- Central Intelligence Agency- În traducere din limba engleză Agenția Centrală de Informații. Este un serviciu secret de informații al Statelor Unite ale Americii ce a fost înființat în anul 1947, avându-l ca fondator pe Harry S. Truman (președinte al Statelor Unite ale Americii la acea vreme).
[17]PLC- Programmable Logic Controller- În traducere din limba engleză controler logic programabil, este un tip de computer minuscul care poate primi date prin intrările sale și poate trimite instrucțiuni de operare prin ieșirile sale.

2010, a atras mult interes media, deoarece a fost primul virus despre care se știe că poate distruge hardware-ul[18]. Potrivit rapoartelor, Stuxnet a provocat arderea unui număr mare de centrifuge de la uzina de îmbogățire a uraniului Natanz din Iran. De-a lungul timpului, alte grupuri au modificat virusul pentru a viza în mod specific infrastructura, cum ar fi liniile de gaz, centralele electrice și instalațiile de tratare a apei. Stuxnet a fost o infecție cu mai multe părți care s-a propagat pe computerele ce rulau sistemul de operare Microsoft Windows și a călătorit pe stick-uri USB[19]. Software-ul Siemens Step 7, folosit de calculatoarele industriale care acționează ca PLC-uri pentru automatizarea și monitorizarea echipamentelor electro-mecanice, a fost căutat de malware-ul de pe fiecare PC infectat. După ce a localizat un computer PLC, atacul malware și-a actualizat codul online și a început să trimită instrucțiuni către echipamentul electro-mecanic de care era responsabil computerul, care ar provoca daune. Virusul a notificat, de asemenea, controlorul principal cu informații incorecte în același timp. Nimeni care urmărea echipamentul nu ar fi știut că există o problemă până când acesta a început să se autodistrugă [21].

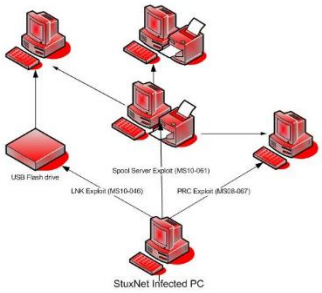


Fig. 15. Viermele Stuxnet
Sursa: https://krebsonsecurity.com/2010/09/stuxnet-worm-far-more-sophisticated-than-previously-thought/

Atacul malware Zeus (cunoscut și sub numele de Zbot), care a apărut pentru prima dată pe internet în 2007, a devenit o infecție foarte eficientă cu cal troian. Multe PC-uri care rulează Microsoft Windows sunt încă în pericol, deoarece malware-ul Zeus și variațiile sale continuă să reprezinte o amenințare serioasă pentru securitatea cibernetică. Deoarece anumite soiuri de viruși Zeus sunt malware fără fișiere, ar putea fi dificil pentru software-ul antivirus să le recunoască. Virusul Zeus poate oferi atacatorilor acces complet la computerele compromise. Multe variante ale virusului Zeus pot fi, de asemenea, utilizate pentru a adăuga ransomware CryptoLocker la un sistem de operare sau pentru a adăuga computere infectate la o rețea bot pentru a efectua atacuri distribuite de refuzare a serviciului (DDoS), în timp ce varianta originală Zeus folosea în principal keylogger-ul[20] browserului pentru a obține acces la acreditările bancare ale unui computer infectat și la alte informații financiare. În 2007, hackerii din Europa de Est au implementat virusul troian Zeus pentru prima dată pentru a ataca Departamentul Transporturilor al SUA. Deși este dificil să identificăm autorul, atacul a luat amploare după ce codul său sursă rău intenționat a fost pus la dispoziția publicului în 2011. De atunci, au apărut multe variații, ținând ocupați atât oamenii legii, cât și specialiștii în securitatea internetului. Infecțiile cu virusul troian Zeus pot pătrunde în sistemele Windows utilizând două rute de atac tipice. Utilizatorii trebuie să viziteze un site web cu codul troian backdoor pentru a se angaja în descărcări drive-by. După aceea, ei descarcă în secret lucruri pe computerul utilizatorului. Browserele moderne, cum ar fi Google Chrome, împiedică în mod obișnuit aceste descărcări și site-urile web pe care se află, dar hackerii vin mereu cu noi modalități de a depăși acest lucru. Pe de altă parte, browserele web mai vechi, cum ar fi Internet Explorer, nu puteau nici măcar să oprească descărcările de tip drive-by. Cealaltă metodă principală de infectare a lui

[18]Hardware- Reprezintă partea fizică a unui sistem informatic.
[19]USB- Universal Serial Bus- În traducere din limba engleză Magistrală Serială Universală reprezintă un standard industrial pentru protocoale de cablare, conectori și comunicații care sunt utilizate pentru a conecta, comunica și alimenta diferite dispozitive de calcul cu energie electrică. [41]
[20] Keylogger- Keylogger-urile sunt un tip de spyware deosebit de insidios care poate înregistra și fura apăsări consecutive de taste (și multe altele) pe care utilizatorul le introduce pe un dispozitiv. [42]

Zeus este atacurile de tip phishing, în care victimele fac clic pe linkuri din e-mailurile de phishing sau postări de pe rețelele de socializare sub impresia că instalează software sigur. Calul troian Zeus are două obiective principale: furtul informațiilor financiare ale utilizatorilor și conectarea computerelor la o rețea bot. Majoritatea variantelor Zeus încearcă să prevină deteriorarea pe termen lung a dispozitivelor pe care le infectează, spre deosebire de multe alte forme de malware. Scopul lor este de a preveni detectarea software-ului antivirus. Atacurile mai lungi cresc probabilitatea ca un hacker să obțină informații utile de la instituțiile financiare. Virusul Zeus este adaptabil și ascuns și, deoarece codul său sursă este disponibil pentru toată lumea, persoanele rău intenționate îl pot modifica cu ușurință pentru a se potrivi scopurilor lor. Cele mai tipice variații Zeus includ:

- Cea mai periculoasă variantă Zeus, Gameover Zeus, permite oricui o folosește să efectueze un atac ransomware potențial catastrofal asupra unui calculator ce rulează Microsoft Windows.
- SpyEye: Acest virus bancar funcționează similar cu malware-ul Zeus, iar cele două programe au multe asemănări.
- Ice IX: Sistemul Ice IX a fost primul botnet construit folosind codul sursă al virusului Zeus după ce a fost făcut public. Pentru a fura date financiare, inclusiv acreditări bancare, utilizează formulare necinstite.
- Carberp: Sistemele de operare Windows XP și Windows 7 sunt afectate de acest malware financiar. Virusul „Zberp" a fost produs prin combinarea acestui troian bancar cu codul de bază Zeus.
- Shylock: Informațiile din conturile bancare sunt, de asemenea, furate de această infecție cu malware prin atacuri de tip man-in-the-browser[21].

Cele mai bune două strategii pentru a proteja dispozitivele împotriva lui Zeus și a mai multor versiuni ale sale sunt implementarea unei securități robuste a punctelor terminale și menținerea programului antivirus la zi.
Semnele că un sistem a fost infectat cu un troian Zeus includ:

- O încetinire bruscă a vitezei de calcul și de procesare a sistemului;
- Tranzacții neobișnuite în aplicațiile bancare;
- Programe necunoscute ce rulează pe SO[22];
- Componentele hardware ale sistemului încep să se încălzească neobișnuit de mult.

Un atac de acest tip este totuși o amenințare, chiar dacă are un lung istoric în spate. De exemplu, în ciuda faptului că atacurile de buffer overflow sunt disponibile de aproximativ 40 de ani, ele pot distruge în continuare serverele și sistemele care nu reușesc să acorde prioritate securității cibernetice. Metodele folosite de persoanele rău intenționate pentru a accesa tehnologia se schimbă așa cum o face tehnologia în sine. În plus, infrastructura societății noastre devine din ce în ce mai computerizată. Ca urmare a acestui fapt, mizele sunt acum semnificativ mai mari.

Când FBI a luat măsuri împotriva Gameover Zeus în 2014, au calculat că virusul infectase deja până la un milion de dispozitive informatice, 25% dintre ele fiind în SUA. Acest lucru a dus la pierderi financiare de peste 100 de milioane de dolari. Pierderea financiară care apare în urma furării acreditărilor bancare este cel mai mare risc imediat de infecție cu Zeus. Atacatorul va beneficia mai mult dacă poate găsi o victimă cu un cont bancar consistent.

Celălalt risc principal al troianului Zeus este mai puțin evident. Atunci când rețeaua botnet are nevoie de computer, infecția și versiunile sale pot rămâne nedescoperite pe acesta luni sau chiar mai mult. Spre deosebire de multe alte tipuri de rețele bot, acestuia îi lipsește un computer de comandă centralizat pe care autoritățile să îl poată identifica și mai apoi să îl; în schimb, orice computer poate furniza directive în orice moment. [22]

[21] Atacul Man-in-the-Browser folosește aceeași strategie ca și atacul Man-in-the-Middle, cu excepția cazului în care un cal troian este folosit pentru a intercepta și modifica apelurile din mers între executabilul aplicației primare (de exemplu de exemplu, browserul) și mecanismele sau bibliotecile sale de securitate.
[22] SO- Sistem de operare

În anul 2011, giganta corporație Sony a anunțat că în cursul a doar câteva zile infractorii cibernetici au reușit să fure informațiile a circa 77 de milioane de utilizatori ai rețelelor PlayStation. Pentru a remedia această problemă experții în securitate cibernetică de la Sony au avut nevoie de 23 de zile pentru a recupera accesul la sistem și a remedia problema.

Doi ani mai târziu, un alt gigantic american din industria comerțului, Target, a fost vizat de un atac de tip phishing. În acest fel, datele bancare a peste 110 milioane de clienți Target au fost furate prin intermediul unui email ce conținea un malware.

WannaCry, probabil cea mai vicleană variantă de ransomware, a reușit să infecteze în anul 2017 peste 200.000 de computere Windows din 150 de țări. Având în vedere că Spitalele Serviciului Național de Sănătate din Marea Britanie au fost printre cele mai grav afectate, a fost deosebit de periculos și fatal. Se crede în mare măsură că infractorii cibernetici nord-coreeni au fost responsabili pentru atac.

Agenția de securitate socială din Costa Rica a fost închisă de un atac ransomware la sfârșitul lunii mai. Atacul s-a extins la alte birouri din țară și a dus la instaurarea stării de urgență în Costa Rica. Acesta este unul dintre cele mai înfricoșătoare exemple ale dorinței infractorilor cibernetici de a pune în pericol viețile și mijloacele de trai ale oamenilor. [16]

2.3. Clasificarea atacurilor cibernetice

Spațiul virtual sau cibernetic este un set de mijloace și proceduri care provin din tehnologia informației și comunicațiilor (TIC). Spațiul virtual sau cibernetic este compus din hardware, software, internet, servicii de informare și sisteme de control. Această infrastructură este esențială pentru activitatea socioeconomică a oricărei națiuni, organizație sau proiect internațional.

Există două grupe principale de amenințări la adresa spațiului cibernetic:

- Amenințările ce privesc informațiile și comunicațiile din spațiul cibernetic;
- Amenințările ce privesc infrastructura din spatele spațiului cibernetic.

Prima grupă, a amenințărilor ce privesc informațiile și comunicațiile au ca și consecințe pierderea, furtul, utilizarea necorespunzătoare și neautorizată a informațiilor. Principalele amenințări ce se înscriu în această categorie sunt:

- Furtul/ publicarea informațiilor personale;
- Furtul/ publicarea informațiilor clasificate sau secrete;
- Furtul de identitate (este vorba de identitatea digitală a indivizilor);
- Frauda cibernetică;
- Spionajul industrial sau de stat.

Din cea de-a doua categorie de amenințări, amenințările la adresa infrastructurii Tehnologiei Informației și Comunicațiilor fac parte din amenințările ce au ca scop întreruperea (fie ea temporală, parțială sau totală) a sistemelor și proceselor din spatele acestora. Din această categorie pot fi identificate următoarele amenințări:

- Atacurile asupra sistemelor Hardware/Software;
- Atacurile asupra serviciilor de internet;
- Atacurile asupra rețelelor sau a sistemelor prin implicarea unor terți;
- Atacurile ce utilizează viermi sau viruși informatici.

Atacurile cibernetice sunt clasificate în principal după două criterii, sursa de proveniență a acestora și impactul pe care îl au. În funcție de aceste două caracteristici atacurile pot fi:

- *Atacuri sponsorizate de state*- în ultimii ani conflictele fizice dintre state s-au mutat în spațiul virtual ducând astfel la apariția unor atacuri cibernetice ce au în spate conducerea anumitor state. Acestea sunt realizate deobicei asupra infrastructurii critice

ale statelor vizate dar și asupra unor obiective specifice. Ca exemplu al unor atacuri de acest fel putem observa atacul cibernetic lansat de Rusia împotriva Georgiei în anul 2008, un atac ce a fost succedat de invazia terestră a Rusiei; atacurile cibernetice asupra rețelelor clasificate ale Guvernului Statelor Unite ale Americii lansate de hackerii chinezi și multe alte exemple ce se încadrează în categoria atacurilor sponsorizate de state. Dezvoltarea amenințărilor avasnate peristente (AAP) a trezit un real interes pentru state în ultimii ani. Atacurile AAP sunt lansate asupra unor obiective foarte specifice, cu rolul de a menține o prezență constantă în rețelele infectate, principalele caracteristici ale acestora fiind agresivitatea crescută cu care atacă sistemele și capacitatea acestora de a se infiltra și de a rămâne în sistem fără a rămâne detectate.

- *Atacuri sponsorizate de către organizații private*- Multe organizații private încearcă să obțină informații economice și industriale de la alte organizații concurente; acest tip de atac este adesea efectuat cu ajutorul guvernului.
- *Terorism, extremism politic și/sau ideologic*- Grupurile extremiste și terorismul folosesc spațiul cibernetic pentru a planifica și publica acțiunile lor și pentru a racola adepți pentru a le efectua. Aceste grupuri sunt conștiente de importanța strategică și tactică an internetului pentru interesele lor, iar forumurile și reţelele sociale au devenit principalul instrument folosit.
- *Atacurile grupurilor de crimă organizată*- Bandele informatice, sau bandele de crimă organizată, au început să își desfășoare activitatea pe internet, profitând de anonimat. Obiectivul acestor bande este de an obține informații sensibile pentru a le folosi pentru fraudă și a câștiga bani.
- *Hackerii*[23]- Odată cu apariția internetului, dar mai ales în ultimii ani, activitatea hackerilor a devenit unul dintre cele mai mari pericole pentru guverne și organizații. Principiile acestei agresiuni sunt anonimatul și transmiterea gratuită de informații prin spațiul cibernetic, în special prin internet. Misiunea lor este de a „ataca" spațiul cibernetic al persoanelor, companiilor, proiectelor sau alte organizații care încalcă interesele sau principiile lor. Acest lucru înseamnă că hackerii pot hackui spațiul cibernetic al guvernelor din majoritatea țărilor din lume, al băncilor, al companiilor de telecomunicații, al furnizorilor de infrastructură critică, al furnizorilor de servicii de internet și, în cele din urmă, al întregului spațiu cibernetic. Obiectivul principal al acestor hackuri este furtul de date sensibile.
- *Atacurile personalului cu acces privilegiat (cei din interior)*- Aceste grupuri reprezintă una dintre cele mai mari amenințări la adresa securității spațiului cibernetic al națiunilor, companiilor și proiectelor, deoarece acestea sunt de multe ori componente esențiale ale tuturor atacurilor menționate mai sus. Aceste atacuri pot include spioni infiltrați de stat, angajați nemulțumiți, bande de teroriști sau infractori cibernetici.

Spațiul virtual sau cibernetic este compus din trei niveluri principale: un nivel fizic, un nivel logic și un nivel social. Fiecare dintre aceste niveluri este alcătuit din cinci părți distincte: componentele geografice, fizice, logice și cibernetice ale rețelei, oamenii și identitățile cibernetice. Nivelul fizic conține componenta geografică și componenta fizică a rețelei. Nivelul logic este reprezentat de componenta logică a rețelei. Ultimul nivel, cel social are în componența sa interfețele și identitățile cibernetice.

Aspectele geografice și fizice ale rețelelor formează stratul fizic. Componenta geografică descrie locația fizică a componentelor fizice ale rețelelor. Componenta fizică a unei rețele este compusă din infrastructură și hardware care ajută rețelele și conectorii fizici cum ar fi cablurile, routerele, serverele și calculatoarele.

Nivelul logic este alcătuit din conexiunile logice care există între nodurile rețelei; un nod poate fi orice dispozitiv conectat la rețeaua, precum și sistemele IT.

[23] Hacker- Persoană care încearcă să obțină, în mod ilegal, controlul unui sistem de securitate, computer sau rețea, cu scopul de a avea acces la informații confidențiale sau avantaje materiale [43].

Oamenii și identitățile cibernetice formează stratul social. Personajele care interacționează în spațiul cibernetic constituie componenta „oameni”. O persoană poate avea unul sau mai multe identități cibernetice și o identitate cibernetică poate fi utilizată de una sau mai multe persoane, deoarece relația dintre oameni și identități cibernetice este de la 1 la n sau de la 1 la 1. Aceste identități online pot fi reale sau false, ceea ce face dificilă urmărirea comportamentului infracțional care are loc pe internet și permite utilizatorului să se bucure de anonimat. Identitățile cibernetice includ profiluri de social media, conturi de utilizator de rețea, conturi de email și altele [23].

Atacurile cibernetice au ca scop distrugerea sau obținerea controlului sau accesului la documente și sisteme vitale dintr-o rețea de computere personale sau de afaceri. Atacurile cibernetice sunt comise de persoane sau organizații cu scopuri politice, infracționale sau personale pentru a distruge sau a obține acces la informații clasificate. Cele mai întâlnite atacuri cibernetice în mediul digital sunt:

- Malware;
- Atacul distribuit de refuzare a serviciilor (DdoS);
- Phishing;
- Atacuri de injectare SQL;
- Scriptare între site-uri (XSS);
- Botnet;
- Ransomware. [24]

Software-ul cunoscut sub numele de malware este conceput pentru a afecta interesele proprietarului unui sistem sau dispozitiv. În timp ce unele tipuri necesită să fie „plantate” pe dispozitiv altele pot ajunge singure acolo. Cum funcționează malware-ul? Efectele sale variază ca severitate, de la urmărirea datelor puțin periculoase până la blocarea dispozitivului pentru a fi răscumpărat sau distrus pentru distracție. Malware-ul există sub o multitudine de forme și varietăți, cele mai frecvent întâlnite și utilizate malware-uri sunt:

- *Adware*- este un tip de software rău intenționat care nu este foarte dăunător și are scopul de a câștiga bani în loc să dăuneze computerului. Acest program bazat pe reclame agresive afișează bannere pe site-uri web și ferestre de aplicații. Anunțurile de tip pop-up sunt cel mai semnificativ simptom. Este posibil ca acestea să apară pe desktop sau în aplicații, programe sau site-uri web care nu le aveau anterior.
- *Spyware*- este creat pentru a urmări acțiunile victimei. Acest tip de malware funcționează în secret, urmărind utilizarea computerului și navigarea pe internet. Poate aduna parole, informații bancare și e-mailuri și chiar poate urmări ce taste sunt apăsate sau poate modifica setările de securitate. Un utilizator la distanță primește toate datele colectate. În plus, are capacitatea de a descărca și instala aplicații dăunătoare fără permisiunea utilizatorului.
- *Viruși*- un virus de calculator se va răspândi de la gazdă la gazdă, la fel ca un virus biologic, pentru a infecta cât mai multe dispozitive posibil. Acesta se poate răspândi prin descărcare, e-mail, rețele sociale sau mesaje text odată ce este atașat la fișiere sau programe. Cu toate acestea, un virus nu poate infecta un computer în mod independent, ci necesită ca un utilizator să execute programul asociat. Virușii pot provoca disconforturi minore, cum ar fi schimbări ale fundalului de pe desktop, până la probleme grave ale sistemului sau pierderea completă a datelor.
- *Viermi*- viermii pot părea destul de inofensivi, în comparație cu virușii, deoarece nu afectează direct sistemele. Un vierme are scopul de a se copia și de a se răspândi într-o rețea sau pe o unitate locală. Viermii pot fi, de asemenea, asociați cu „sarcini” care au scopul de a dauna unui sistem sau de a extrage date; cu toate acestea, acestea nu fac întotdeauna acest lucru. Creeper, primul vierme, pur și simplu și-a informat utilizatorii infectați că există.
- *Troieni*- malware-ul de tip troian se infiltrează în computere ascunzându-se în programe care par să nu fie dăunătoare, asemănătoare calului troian din legenda greacă. Atunci când a intrat, poate crea căi de acces pentru hackeri pentru a pătrunde în sistem. și a

colecta datele sau chiar pentru a bloca complet accesul la computer. De exemplu, troianul Zeus despre care am discutat în subcapitolul anterior, colectează informații despre victime, cum ar fi apăsările de taste și identificarea victimelor. Emotet este renumit pentru furtul de date de la persoane și companii.

- *Ransomware*- datorită capacității sale de a se răspândi rapid și de a provoca daune costisitoare, ransomware-ul este una dintre cele mai grave amenințări cibernetice. Ransomware-ul funcționează pentru a câștiga bani. Malware-ul infectează un dispozitiv folosind o vulnerabilitate a sistemului și criptează toate datele, ceea ce blochează accesul utilizatorului. Apoi cere victimei să plătească pentru decriptarea fișierelor.
- *Keylogger*- programele keylogger pot fi hardware sau stalkerware[24]. Acest lucru le poate face extrem de dificil de identificat. Ele au ca scop urmărirea tastelor ce sunt apăsate de utilizator.

Cele mai comune metode de răspândire a programelor de tip malware sunt:

- *E-mail*- cea mai frecventă modalitate prin care virușii se răspândesc este prin e-mail. Atât atacurile de tip phishing sofisticate, cât și atacurile de tip spam simple continuă să păcălească oamenii să dea clic pe linkuri sau să descarce atașamente care conțin malware;
- *Navigare neglijentă*- există o mare probabilitate să ajungeți pe un site web neintenționat dacă faceți clic pe orice pop-up sau anunț pe care îl vedeți în timp ce navigați pe internet. Acesta va descărca automat un malware în fundal și se va prinde pe dispozitiv cu un keylogger sau un troian;
- *Colegi de serviciu*- unele programe malware se răspândesc prin rețeaua internă. De exemplu, un angajat din birou a trecut cu vederea instrucțiunile de securitate cibernetică și a dat clic pe un link care a fost făcut rău intenționat. A doua zi, fiecare computer a fost infectat și fișierele au fost criptate, astfel încât nimeni nu mai putea accesa conturile;
- *Pachete de software*- malware-ul are capacitatea de a se răspândi prin alte programe. Există probabilitatea să existe câteva surprize chiar și atunci când se descarcă un software de încredere. După ce software-ul legitim este instalat, se poate instala și un malware, care poate fi de la un adware ușor enervant până la un spyware care poate fura datele bancare, fără ca victima să își dea seama.

Semnele infectării cu un malware sunt deobicei reprezentate de modificări ale vitezei de procesare (fie vorbim de viteza browserului, fie de cea a dispozitivului), blocări ale dispozitivului sau chiar închideri nejustificate ale acestuia, comportament ciudat al aplicațiilor deja existente (acestea se închid/deschid automat), apariția unor aplicații sau a unor programe necunoscute pe dispozitivul infectat, modificări ale setărilor în ceea ce privește securitatea dispozitivului, trimiterea unor mesaje sau a unor e-mailuri în mod automat, fără acceptul victimei, și nu în ultimul rând efectuarea unor plăți suspecte efectuate din conturile victimei. [25]

Adware (fig. 16) este un tip de software bazat pe anunțuri publicitare care permite dezvoltatorilor să ofere publicului produsele lor fără costuri, dar totuși să primească bani de la o companie de publicitate. În schimbul unei sume de bani, dezvoltatorul fie va combina coduri care vor afișa reclame în rețeaua de publicitate, fie va convinge utilizatorul să instaleze software de la un alt furnizor alături de produsul original. Adware-ul poate fi dăunător. Distincția între adware și spyware este atât de subtilă încât multe victime nici nu realizează că au fost victimele acestui tip de atac cibernetic. Anunțurile, care pot fi formate din ferestre pop-up sau videoclipuri, nu ar trebui să fie o problemă la început. Cu toate acestea, în spatele lor se poate ascunde un program suspect care poate urmări activitățile utilizatorului, creând un model al obiceiurilor sale de navigare sau încurajându-l să achiziționeze un produs printr-o rețea afiliată.

[24] Stalkerware- Un program sau o aplicație de supraveghere cunoscută sub numele de stalkerware permite altcuiva să urmărească dispozitivul. De obicei, este introdus fără știrea sau aprobarea proprietarului. Stalkerware-ul poate fi inclus cu un software sau o aplicație care a fost instalată de bună voie sau poate fi plasat pe dispozitiv cu intenții rele. [44]

Fig. 16 Atac de tip Adware
Sursa: https://www.techtarget.com/searchsecurity/definition/adware

Există cu siguranță controverse cu privire la software-ul bazat pe reclame, deoarece unele dispozitive precum e-book, telefoanele mobile și aplicațiile de mesagerie includ acest tip de program și solicită consimțământul utilizatorului pentru an obține anumite beneficii. Termeni și condiții sau contractul de licență al utilizatorului final pot conține informații despre adware, dar de cele mai multe ori acesta nu este citit cu atenție și astfel se ajunge în situația în care adware-ul să fie folosit cu acordul utilizatorului. Adware-ul a atacat până acum mai multe aplicații cunoscute și de încredere într-o manieră dăunătoare și agresivă. [26]

Toate aplicațiile care trimit date private fără consimțământul sau știința utilizatorului se încadrează în categoria de Spyware. Aplicațiile spyware trimit date statistice, cum ar fi liste de site-uri web vizitate, adrese de email din lista de contacte a utilizatorului sau liste de apăsări de taste înregistrate. Atacatorii ce folosesc spyware susțin că aceste metode urmăresc să înțeleagă mai bine dorințele și nevoile utilizatorilor pentru a permite reclame mai țintite. Problema este că nu există o distincție clară între aplicațiile utile și cele dăunătoare. De asemenea, nimeni nu poate fi sigur că datele recuperate nu vor fi utilizate incorect. Aplicațiile spyware pot colecta date precum coduri de securitate, coduri PIN[25] și numere de conturi bancare. Aplicațiile spyware sunt adesea încorporate în versiuni gratuite ale programelor de către creatorii acestora pentru a obține bani sau pentru a motiva utilizatorii să cumpere software. Aplicațiile client pentru rețelele peer-to-peer[26] sunt un exemplu de freeware bine cunoscute care sunt împachetate cu spyware. Aplicații precum Spyfalcon și Spy Sheriff sunt incluse într-o subcategorie specială de spyware care pare a fi programe antispyware, dar în realitate sunt programe spyware. Programele de înregistrare a apăsărilor de taste, o subcategorie a spyware, pot fi bazate pe soluții hardware sau software. Programele bazate pe software pentru înregistrare a apăsărilor de taste pot colecta doar date tastate într-un singur site web sau aplicație. Programele de înregistrare a apăsărilor de taste mai avansate pot înregistra orice tastare, inclusiv datele de tip ,,copy-paste". Unele aplicații pentru înregistrare a apăsărilor de taste pe dispozitivele mobile pot înregistra apeluri, informații din aplicațiile de mesagerie, locații sau chiar capturi de cameră și microfon [27]. Unul dintre cele mai comune tipuri de spyware este înregistrarea caracterelor introduse cu tastatură. Acest lucru, cunoscut și sub numele de keylogger, înregistrează fiecare tastă apăsată pentru a fura parolele și alte date sensibile. Multe persoane folosesc stickuri USB (fig. 17) fără să le verifice, ceea ce face ca USB keyloggerul să fie o problemă răspândită. În alte situații, deținătorii instalează spyware-ul deliberat în rețele comune sau publice pentru a monitoriza activitatea și a preveni breșele de securitate. Guvernele din întreaga lume folosesc sau creează propriul software de spyware, în afară de companiile care doresc să monitorizeze activitatea angajaților, pentru a ataca potențialele amenințări la securitatea națională și pentru a combate terorismul. În

[25] PIN- Personal Identification Number sau în traducere din limba engleză număr de identificare personală, este un cod de acces format din patru cifre.
[26] Peer-to-peer (P2P)- se referă la rețelele de calculatoare ce utilizează o arhitectură distribuită. Toate dispozitivele compenente ale acestui tip de rețea își împart între ele sarcinile.

prezent, este discutat despre al doilea scop pentru care este folosit spyware-ul. Acest lucru s-a întâmplat după ce organizația internațională pentru drepturile omului, Amnesty International, s-a opus în 2015 practicii guvernului de a spiona jurnaliști și activiști pentru drepturile omului, considerând-o un atac la libertatea de exprimare. Cu toate acestea, nu toate programele de spyware sunt folosite cu rea intenție. Unele programe sau rețele de socializare legitime, cum ar fi Facebook, sunt echipate cu spyware pe care îl acceptăm fără să ne dăm seama și îi permit să analizeze activitatea utilizatorului și să afișeze anunțuri direcționate. [28]

Fig. 17 Stick USB- unul din principalii purtători de keylogger
Sursa: https://www.distrelec.ro/ro/usb-stick-pinstripe-64gb-usb-black-verbatim-49065/p/11055081

Virusul informatic sau de calculator este un program de tip software care, deși nu este foarte mare ca dimensiune, se poate răspândi ușor de la un dispozitiv la altul și de la un fisier la altul, provocând probleme de funcționare dispozitivului infectat. Virușii informatici pot modifica sau șterge datele de pe dispozitiv, cel mai facil mod de transmitere al acestora fiind prin intermediul e-mailurilor. Un virus informatic poate fi transmis și prin mesaje instantanee sau link-uri dacă utilizatorul le activează fără să realizeze consecințele. De aceea, nu este recomandat să deschizi mesaje și e-mailuri decât dacă expeditorul este cunoscut. Poate veni în diferite forme, cum ar fi imagini, fisiere video sau audio, linkuri, felicitari, GIF-uri[27] și alte variante. De asemenea, poate fi ascuns în programele descarcate de pe internet în mod obișnuit sau în mod fraudulos. Cum se comportă virușii? Se instalează automat pe dispozitivul infectat fără permisiunea utilizatorului și încep să atace componentele hardware sau software ale dispozitivului, ceea ce are potențialul de a distruge computerul. [29]

Cel mai important criteriu de clasificare al virușilor informatici este după componenta pe care aceștia o afectează. Astfel, putem vorbi despre existența a două mari categorii, și anume: viruși hardware și viruși software. Virușii hardware sunt cei care afectează componentele fizice ale dispozitivului, componente precum hard disk-ul[28], procesorul sau memoria RAM[29] a unui dispozitiv. Cea de-a doua categorie este cea a virușilor software, viruși ce afectează fișierele și programele aflate în memoria dispozitivului. În plus, acești tipi de virus afectează inclusiv sistemul de operare al dispozitivului și componentele acestuia. Principalele efecte cauzate de infectarea cu un virus ce atacă partea software sunt:

- Ștergerea tuturor informațiilor și datelor stocate în memoria dispozitivului;
- Formatarea hard disk-ului;
- Distrugerea unor fișiere sau a tabelelor de alocare (ducând asftel la incapacitatea citirii datelor de pe disc);
- Modificarea dimensiunilor unor fișiere;

[27] GIF- aconim pentru Graphics Interchange Format- reprezintă o serie de animații ce se repetă la infinit cu o viteză mare.
[28] Hard disk- cunoscut în limba română ca și „discul dur” sau „discul rigid”, este o componentă fizică ce are ca scop stocarea datelor sau memorarea nevolatilă a acestora.
[29] Memoria RAM- componentă fizică a unui dispozitiv ce are ca scop stocarea volatilă a datelor. Prin volatilitatea stocării datelor se înțelege că datele stocate sunt pierdute în momentul în care dispozitivul este oprit. Denumirea sa vine din limba engleză, RAM fiind abrevierea de la Random Access Memory (Memorie cu Acces Aleatoriu). Se poate afirma astfel că memoria RAM este o „memorie pe termen scurt”.

- Scăderea vitezei de lucru al dispozitivului (în cazuri extreme această scădere duce la închiderea dispozitivului);
- Ascunderea fișierelor și blocarea acestora de la a fi accesate.

O altă metodă de a clasifica virușii este în funcție de programul în care aceștia se infiltrează (vorbim aici de programe executabile). Având în vedere acest tip de clasificare virușii pot fi:

- *Viruși MBR*[30]- sunt virușii care infectează MBR-ul unui hard disk. MBR-ul este sectorul care conține un program scurt ce are ca scop încărcarea sistemului de operare. Sistemul de operare nu se mai poate încărca dacă acest sector este deteriorat.
- *Viruși BS*[31]- Virușii BS țintesc dischetele, CD-urile[32] sau DVD-urile(fig. 18) [33], dar sunt asemănători cu virușii MBR;

Fig. 18 Mediu de stocare- DVD
Sursa: https://www.indiamart.com/proddetail/audio-video-blank-dvd-9894454362.html

- *Viruși de fișiere*- sunt virușii care infectează o categorie specifică de fișiere. Fișierele executabile (fișierele ce au extensia .EXE sau .COM), fișierele overlay (fișierele ce au extensia .OVL) și fișierele de sistem (fișierele ce au extensia .SYS sau .DRV) sunt cele mai frecvent infectate.
- *Viruși de macro-uri* - virușii sunt plasați într-unul sau mai multe macro-uri din documentele Microsoft Office[34] și folosesc caracteristicile VBA[35].
- *Viruși pereche*- sunt virușii care creează un nou fișier executabil cu un nume identic dar extensie diferită (de tipul .COM). În cazul în care două fișiere executabile au denumiri identice, dar au extensii diferite .COM și extensia .EXE sunt lansate inițial de sistemul de operare Microsoft Windows fișierele cu extensia .COM.
- Virușii de link-uri- sunt virușii care modifică structura directorului unui fișier infectat, redirecționând directorul către locația virusului. După lansare, virusul poate citi calea directorului fișierului și poate încărca fișierul executabil.
- Viruși specifici- sunt virușii ce acționează asupra unei aplicații alese. Cei mai cunoscuți viruși de acest tip sunt virușii de ActiveX (viruși creați pentru a ataca produsele

[30] MBR- abreviere de la Master Boot Record reprezintă vechiul standard de administrare a partițiilor pe hard disc pe 32 biți. Aici este stocat codul executabil care încarcă sistemul de operare, precum și informațiile despre organizarea partițiilor. IBM a dezvoltat MBR în 1983 și este încă folosit. [45]
[31] BS- abreviere de la Boot Sector. Un sector de boot există pe o unitate de hard disk internă, unde este instalat Windows, precum și pe dispozitive de stocare care nu necesită încărcare, dar care transportă doar date personale, cum ar fi un hard disk extern, o dischetă sau un alt dispozitiv USB. [46]
[32] CD- abreviere de la Compact Disk sau în limba română disc compact
[33] DVD- abreviere de la Digital Video Disc sau Digital Versatile Disc, este un mediu de stocare optic ce a fost creat pentru a succede CD-urile ale căror capacitate de stocare devenise prea mică pentru cerințele acelor vremuri.
[34] Microsoft Office- este o colecție de aplicații desktop de productivitate care a fost special concepută pentru utilizarea în tot ceea ce înseamnă muncă la birou sau afaceri. A fost lansat în 1990 și este un produs al companiei americane Microsoft. Această colecție de aplicații conține programe precum Word, Excel, PowerPoint, Access, OneNote, Outlook și Publisher.
[35] VBA- acronim pentru Visual Basic for Applications, reprezintă codul de programare la care utilizatorii Microsoft Excel au acces (pentru a-l citi și modifica) atunci când doresc să creeze macro-uri în aplicația Excel.

companiei Microsoft utilizând un cod ce a fost în prealabil încărcat pe un server), virușii VB script (folosesc Visual Basic pentru a accesa codul dăunător de pe un server web și a-l distribui în stațiile de lucru locale, accesul la o pagină web fiind suficient pentru a infecta sistemul local de operare) și virușii de Java[36] (se folosesc de programele Java pentru a realiza acțiuni neautorizate pe stațiile de lucru).

Din punct de vedere al modului de funcționare și a tehnicilor folosite virușii se pot împărți în 3 categorii:

- *Virușii invizibili*- potrivit unui articol de pe site-ul wowhost.ro acest tip de viruși ,, folosesc tehnici de mascare care ascund faptul că sistemul a fost infectat. Când sistemul de operare încearcă să afle dimensiunea unui program infectat, virusul ascuns scade o parte din aceste date, egală cu dimensiunea propriului cod şi o înlocuieşte cu datele corecte. Astfel, dacă programul este doar citit de un scanner de viruşi, dar nu este rulat, codul viral este ascuns şi nu poate fi detectat.” ;
- *Viruși polimorfici*- folosesc metode de criptare sofisticate pentru a-și modifica codul viral. Acest tip de modificare este cunoscut sub numele de mutație. Un virus își poate modifica dimensiunea și compoziția prin mutație. În plus, programele antivirus îi pot recunoaște cu dificultate datorită modificării semnăturii, ceea ce îi face mult mai greu de detectat;
- *Viruși rezidenți în memoria dispozitivului*- se instalează rapid în memorie RAM pentru a se ataşa fişierelor executabile sau documentelor Microsoft Office deschise. Acești viruși au capacitatea de a controla întregul sistem și au capacitatea de a îl infecta oricând;
- *Viruși non-rezidenți în memoria dispozitivului*- aceştia sunt activați doar de pornirea aplicației infectate. [30]

Termenul „vierme informatic” sau „worm” se referă la un tip de amenințare cibernetică care se poate replica și se răspândește automat într-o rețea. Viermii informatici sunt asemeni virușilor programe care sunt menite să provoace probleme de funcționare sau chiar distrugeri de date prin rețelele de comunicare dintre calculatoare. Ei sunt capabili să se înmulțească și sunt similare troijenilor, deoarece nu atacă doar fișiere, ci întregul sistem, funcționează independent și folosește resursele dispozitivului-gazdă. În consecință,viermii sunt un tip de malware, sau software rău intenționat, care pare a fi inofensiv deoarece ocupă doar o parte din lățimea de bandă. Orice tip de program invaziv și ostil care funcționează fără permisiune este în general acoperit de termenul de vierme informatic.

O clasificare a viermilor informatici se poate realiza în funcție de modul acestora de răspândire:

- *Viermi de internet*- pentru a putea intra în contact cu resursele și vulnerabilitățile rețelei, verifică toate resursele și vulnerabilitățile computerului. O abordare mai comună este să găsească computere care nu au instalate încă ultimele actualizari de securitate și să le trimită pachete de actualizare care includ însuși viermele sau un mic program utilitar care va instala viermele;
- *Viermi de e-mail*- se răspândesc prin atașamente e-mail sau link-uri către site-uri cu viermi. Vizate sunt serviciile Windows Address Book și MS Outlook, care colectează date despre adrese de e-mail. De asemenea, pot scana și prelua adrese de e-mail din orice fișier care conține informații de acest tip. În plus, acest tip de viermi poate crea noi adrese de e-mail combinând nume de domenii. În figura 19 se poate observa cum arată un e-mail ce conține un astfel de vierme informatic;
- *Viermi de mesagerie*- utilizează mesageria instantanee și infectează pe toată lumea din lista de contacte prin transmiterea link-urilor ce redirecționează victimele pe site-uri infectate;

[36] Java- este un limbaj de programare orientat-obiect (OOP) dezvoltat de James Gosling la Sun Microsystems (acum o filială a Oracle) la începutul anilor '90. A fost lansat pentru prima dată în 1995. [47]

- *Viermi de IRC*[37]- transmite fisiere infectate persoanelor care sunt conectate la un canal de IRC sau link-uri către site-uri infectate;
- *Viermi de sharing*- se copiază singuri sub un nume comun în folderele din rețea și apoi infectează toată rețeaua. [31]

Fig. 19 E-mail ce conține un link infectat cu un vierme informatic
Sursa: https://www.malwarebytes.com/blog/threats/worm

Primul vierme cunoscut a fost construit și lansat în noiembrie 1988 de Robert Tappan Morris, student la informatică la Universitatea Cornell. A fost creat inițial pentru a realiza o numărătoare a computerelor conectate la o rețea și acum este denumit viermele Morris. „The Shockwave Rider", o carte fictivă a lui John Brunner publicată în anul 1975, este locul unde a apărut pentru prima dată denumirea de „vierme informatic". Acest vierme poate extrage date și informații din dispozitivul infectat, ceea ce indică faptul că este mai mult ca un hoț de informații decât un software cu auto-replicare. Chiar dacă la începuturile sale viermele informatic a fost conceput într-o manieră pozitivă, de-a lungul timpului acesta a devenit o unealtă folosită de infractorii cibernetici pentru a fura date, transformându-l astfel într-un software de tip malware. În zilele noastre viermii informatici nu mai reprezintă o amenințare atât de mare la securitatea sistemelor precum o făceau în urmă cu câțiva ani, dar cu toate acestea ei implică o serie de riscuri. Printre cei mai cunoscuți viermi informatici creați de om de-a lungul timpului se numără: Bagle (cunoscut și sub denumirea de Beagle, Mitglieder sau Lodeight), Blaster (cunoscut și ca MSBlast, Lovesan sau Lovsan), Conficker (sau Downup, Downadup sau Kido), Duqu, Flame, ILOVEYOU (cunoscut și sub denumirea de Love Letter), Mydoom, Netsky, Nimda, Samy, Sasser, SQL Slammer, Storm, Stratation și Stuxnet. [32]

Grecii au folosit calului troian pentru a pătrunde în Troia și chiar pentru a-l cuceri. În conformitate cu aceeași analogie, troianul este un program dăunător utilizat de hackeri pentru a obține acces la un computer. În același mod în care calul troian a păcălit locuitorii Troiei, acest troian păcălește utilizatorii pretinzând că este un software autentic. Un troian este un tip de malware care se pretinde a fi o aplicație, o utilitară sau un produs software pentru a păcăli un utilizator și a-l face să îl execute. Spre exemplu, un troian ar putea încerca să păcălească o persoană care încearcă să acceseze conținut video – descărcat de obicei prin rețele P2P – pentru a-l convinge să instaleze un „codec special", care ulterior ar putea servi drept poartă de acces sau un tip de ransomware. Spre deosebire de viruși sau viermi, troienii alcătuiesc cea mai mare parte din malware și nu pot infecta fișiere sau să se răspândească într-o rețea fără intervenția utilizatorului. Aceste aplicații dăunătoare sunt extrem de specializate: pot permite accesul de la distanță la un computer, pot lansa atacuri de tip denial-of-service (DdoS), pot descărca troieni

[37] IRC- este un acronym pentru Internet Relay Chat (în traducere din limba engleză comunicare instantanee prin internet). IRC-ul este un serviciu ce are ca scop transmiterea mesajelor în timp real.

suplimentari pentru alți infractori cibernetici sau pot trimite mailuri spam[38] de la computere infectate. Troienii de acces la distanță (RAT) sunt de obicei populari pe sistemul de operare Android ce este instalat pe dispozitivele mobile, deoarece le permit atacatorilor să folosească aplicații semnificative pentru an exploita vulnerabilitățile sistemului de operare mobil și a prelua controlul. O nouă familie de troieni, ransomware-ul, a apărut pe prima pagină a ziarelor începând cu sfârșitul anului 2014. Ransomware-ul este un tip de malware care criptează datele oamenilor și cere bani în schimbul cheii de decriptare.

Troienii sunt cel mai răspândit tip de malware pe macOS[39] și Windows. De obicei, metodele de livrare a troienilor pe platforme specifice utilizează instrumente de inginerie socială, cum ar fi phishing-ul și spam-ul, site-urile web infectate sau escrocherii care se bazează pe rețelele sociale preferate ale victimei.

Troienii sunt frecvent utilizați împotriva țintelor Windows de profil înalt și rămân pe lista celor mai periculoase amenințări la adresa punctelor terminale Windows din întreaga lume. În ciuda eforturilor globale de a elimina troienii cunoscuți precum Trickbot, Emotet, Dridex și AgentTesla, infractorii cibernetici au continuat să folosească aceste tipuri de malware și în ultimii ani.

O mare parte a infecțiilor cu troieni pe Mac[40] au loc de la site-urile warez, care sunt focare de descărcări piratate. Cu orice vector, troienii reprezintă cea mai mare amenințare pentru Mac-uri, iar cea mai mare parte a acestor atacuri troieni au avut loc în Statele Unite, reprezentând 36% din activitatea troienilor care au vizat macOS la nivel mondial în 2021. Acest lucru nu este o surpriză, având în vedere că Statele Unite au probabil cea mai mare bază de instalare a sistemului de operare macOS din lume.

Sistemul de operare Android este și el vulnerabil la troieni. Cu peste 3 miliarde de dispozitive Android active în lume în 2022, infractorii cibernetici au început să dezvolte amenințări cibernetice și pentru smartphone-urile Android, în ciuda faptului că amenințările au vizat anterior doar Windows și macOS. Troienii de root se numără printre cele mai perfide amenințări, deși troienii care trimit SMS-uri sunt de obicei populari pentru că oferă o modalitate simplă de a face bani. Troienii de bază sunt proiectați pentru a obține controlul complet asupra unui dispozitiv de la distanță, permițând atacatorului să acceseze orice tip de informații stocate, ca și cum ar deține efectiv dispozitivul. În ciuda faptului că unii utilizatori ar putea dori să-și rooteze[41] telefoanele pentru a șterge aplicațiile preinstalate care de obicei nu pot fi eliminate sau chiar pentru a modifica versiunea de Android a dispozitivului, troienii de root sunt adesea instalați fără știrea utilizatorului. De exemplu, troienii au reușit să intre în Google Play[42]. Aplicația s-a dovedit a fi un joc de blocuri de culori complet legitim, care poate fi actualizat cu cod malițios de atacatori. Atunci când o actualizare malițioasă a ajuns pe dispozitiv și an obținut privilegii administrative la nivel de sistem, a avut capacitatea de a instala aplicații potențial malițioase pe dispozitiv în mod ascuns, fără ca utilizatorul să fie conştient. [33]

Termenul de troian a apărut pentru prima dată într-un raport din 1974 al Forțelor Aeriene al Statelor Unite ale Americii, care analiza vulnerabilitățile computerului. Până în 1983, a devenit foarte popular după ce Ken Thompson a folosit această frază în prelegerea cunoscută sub numele de Turing, unde a spus: „În ce măsură ar trebui să aveți încredere în declarația că un program nu conține cai troieni? Poate că este mai important să aveți încredere în: oamenii care au scris software-ul.”

[38] Spam- reprezintă orice tip de comunicare nesolicitată și nedorită. Majoritatea cazurilor de spam au legătură cu trimiterea unor mesaje sau e-mailuri ce au caracter comercial.
[39] macOS- reprezintă sistemul de operare folosit de dispozitivele produse de companie Apple.
[40] Mac- denumirea computerelor produse de compania Apple.
[41] Root-area – este procesul ce permite accesul și modificarea fișierelor, unui dispozitiv ce rulează sistemul de operare Android, care sunt de obicei inaccesibile, cum ar fi cele care sunt stocate pe partiția de sistem. În plus, având acces root, există capacitatea de a rula o clasă nouă de aplicații de la terți producători și de a efectua modificări la nivel de sistem. [48]
[42] Google Play- Serviciile Google Play sunt un software de sistem de bază care permite utilizatorului să folosească toate caracteristicile necesare pe orice dispozitiv Android certificat.

Bulletin Board System, care permitea utilizatorilor să acceseze internetul prin linie telefonică, a contribuit la creșterea malware-ului Troian în anii 1980. Pe măsură ce computerele au devenit din ce în ce mai capabile să încărce, descărce și să partajeze fișiere, malware-ul rău intenționat a fost injectat în sistemele de operare. În prezent, există mii de versiuni ale acestui tip de malware.

Deși Troienii sunt adesea considerați viruși, acest lucru nu este corect din punct de vedere tehnic.Un virus de calculator va încerca să răspândească infecția ori de câte ori este posibil, în timp ce un troian este un program individual care îndeplinește anumite funcții, cum ar fi:

- Rootkit- ascunde anumite activități din sistem.Acest lucru permite malware-ului să funcționeze fără a fi detectat, ceea ce crește durata de timp până când acesta este descoperit și daunele pe care le poate provoca o singură „infecție";
- Backdoor- un Troian backdoor permite infractorilor cibernetici să aibă control total de la distanță asupra fișierelor, permițându-i să editeze, să trimită, să descarce și să șteargă date. Sunt obișnuiți să deturneze dispozitive personale pentru activități criminale;
- Exploatare- exploatează munca folosind o breșă de securitate din software-ul computerului. Acest tip de Cal Troian poate manipula o vulnerabilitate pentru a avea acces direct la fișierele stocate, indiferent dacă este într-o aplicație sau afectează sistemul de operare în sine;
- DdoS- acești Troieni, cunoscuti sub numele de „Denial of Service Distributed", vor cere computerului să trimită o mulțime de cereri la o anumită adresă URL[43] în scopul de a supraîncărca serverul și de a închide site-ul web.
- Spyware- are ca scop să intercepteze datele personale ale utilizatorilor. Obiectivul este atins prin copierea fișierelor sau prin utilizarea unui keylogger sau a unui ecran pentru a înregistra ceea ce este tastat și ce site-uri sunt vizitate;
- Ransomware- de multe ori atacurile de tip ransomware sunt realizate prin folosirea unui troian. Odată ce troianul ajunge pe dispozitiv, el criptează informația ca mai apoi persoana ce se află în spatele atacului să perceapă de la victimă o recompensă în vederea oferirii unei chei de decriptare prin care aceasta să recapete accesul la datele ce au fost afectate.

Deși acestea sunt toate tipuri comune de Troieni, obiectivele lor pot fi foarte diferite.Cele mai multe au scopul de a fura informații cu scopul de a câștiga bani.Acestea pot include date bancare, contacte personale, parole pentru platforme de mesagerie instantanee, informații despre jocuri online și multe altele. [34]

Un alt tip de virus malware este ransomware. Acesta demonstrează prezența sa pe computerele infectate prin limitarea accesului la anumite date sau chiar la întregul echipament. Ransomware este un termen care se referă la recuperarea datelor în schimbul unei răscumpărări. Practic, victimele acestor tipuri de atacuri vor primi un mesaj de avertizare pe ecranul dispozitivului lor, informându-le că nu pot accesa informații importante decât dacă vor plăti o sumă de bani, uneori foarte mică, într-un interval de timp scurt. În cazul în care plata este efectuată, utilizatorul va primi un cod care îi va permite, de obicei, să recupereze datele. Dacă plata nu este efectuată în termenul stabilit, datele vor fi șterse și nu vor mai putea fi accesate. Deoarece plata se face de obicei în monede electronice, cum ar fi Bitcoin, autoritățile pot urmări greu acest tip de fraudă informatică.

În ultimii ani, mai multe tipuri de ransomware au apărut pe computerele oamenilor de pe tot globul. Patru dintre aceste tipuri se disting prin frecvența cu care apar, precum și prin efectele devastatoare pe care le au:

- *Crypto ransomware*- cel mai frecvent tip de ransomware este crypto ransomware, care se manifestă prin blocarea anumitor fișiere din dispozitiv, de obicei imagini sau texte. În caz contrar, informațiile vor fi șterse pentru totdeauna. Accesul va fi permis numai după efectuarea plății răscumpărării. În figura 20 se poate observa mesajul afișat în cazul unui atac de tip Crypto ransomware;

[43] Adresa URL- reprezintă abrevierea de la adresă uniformă pentru localizarea resurselor.

- *Locker ransomware*- deși funcționează la fel ca ransomware-ul de tip crypto, locker-ul blochează dispozitivul în întregime, nu doar anumite fisiere;
- *Scareware ransomware*- Scareware este un tip de virus care generează mesaje false de avertizare despre anumite probleme, mesaje ce nu dispar decât atunci când un anumit program esteutilizat, program pentru care atacatorii solicită o sumă de bani;
- *Doxware*- Doxware este un virus care blochează anumite fisiere și amenință să difuzeze date sensibile, cum ar fi fotografii sau videoclipuri compromițătoare, informații financiare secrete, baze de date ale clienților și multe altele. [35]

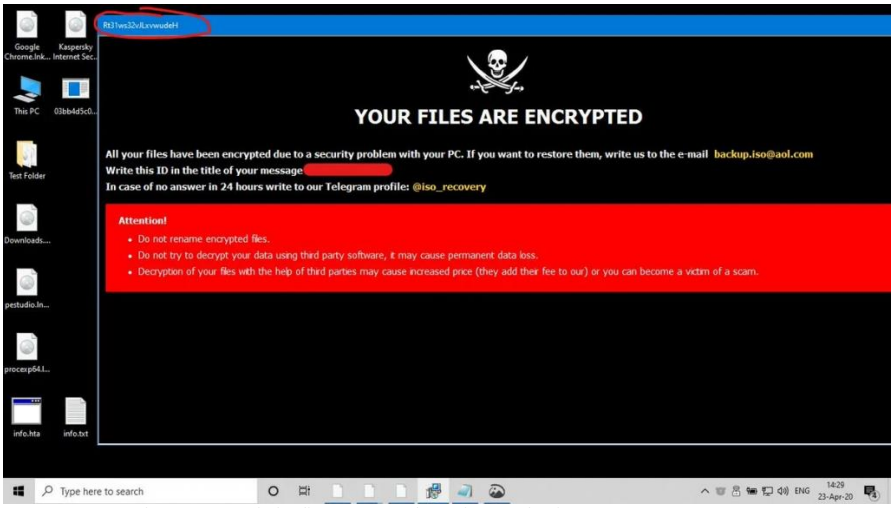


Fig. 20 Mesajul afișat în cazul unui atac de tip crypto ransomware
Sursa: https://www.backblaze.com/blog/complete-guide-ransomware/

În ultimii ani, numărul atacurilor de tip ransomware a înregistrat o creștere exponențială, aducând bani frumoși infractorilor cibernetici ce au stat în spatele acestora. În pasajele ce urmează vom vorbi despre cele mai importante atacuri ransomware petrecute în ultimii ani.

LockERGOGA a fost dezvăluit pentru prima dată în ianuarie 2019 ca un atac cibernetic asupra companiei franceze Altran Technologies, care oferă consultanță în inginerie. Deoarece rețelele sale informatice și toate aplicațiile au căzut, operațiunile companiei în mai multe țări au fost afectate. LockerGoga este livrat și executat de instrumentul PsExec; este un înlocuitor simplu de telnet care poate trece peste câteva verificări de securitate ca software semi-valid. Instalarea duce la deconectarea forțată a sistemului și la modificarea conturilor utilizatorilor pentru sistemul vizat. De asemenea, fișierele de instrumente sunt auto-redenumite și mutate, făcându-le aproape imposibil de găsit. În alte versiuni ale LockerGoga, blocarea este atât de completă încât victimele nu pot vedea nota de răscumpărare sau instrucțiunile de recuperare, chiar dacă cererile sunt îndeplinite. Nu există un decriptor specific care să detecteze și să protejeze sistemele împotriva LockerGoga. În 2019, LockerGogain a vizat, în afară de Altran Technologies, NorskHydro și două companii din industria chimică din SUA și anume Hexion și Momentive.
A fost estimată o pagubă de 50 de milioane de dolari americani (aproximativ 42 de milioane euro) doar pentru atacul asupra NorskHydro.

KAT YUSHA este un troian ransomware care a fost implementat pentru prima dată în octombrie 2018. Acesta criptează fișierele victimei, șterge copiile-umbră și trimite atașamente prin e-mail. Pentru a se răspândi, Katyusha folosește exploit-urile EternalBluean și DoublePulsar. Din păcate, niciun instrument sau decriptor pentru apărare nu este încă disponibil.

JIGSAW criptează fișierele victimei și le șterge, de obicei în 24 de ore, dacă cererile nu sunt îndeplinite. Mai mult, rata de ștergere crește dacă victima încearcă să-și închidă calculatorul, de exemplu. Acest ransomware a fost numit după un personaj din filme horror. Cu toate acestea, companiile de securitate produc actualizari regulate pentru un decriptor Jigsaw eficient.

PewCRYPT a fost lansat la începutul anului 2019 și, spre deosebire de majoritatea programelor ransomware, are doar scopul de a forța utilizatorii să se aboneze la canalul de YouTube al lui PewDiePie. PewDiePie (un youtuber suedez) a concurat cu T-Series, un canal de Bollywood indian, și fanii săi au decis să folosească PewCrypt pentru a-și ajuta idolul să câștige lupta ce avea ca scop să ajungă canalul cu cel mai mare număr de abonați de pe platforma YouTube. PewCrypt este un ransomware care este frecvent răspândit prin mesaje de înșelăciune și reclame online rău intenționate. A fost dezvoltat în Java. Un instrument de decriptare a fost lansat chiar de către autor în martie 2019.

RYUK a apărut pentru prima dată în august 2018 și a fost susținut că are legături cu grupurile de hacking nord-coreene. În curând, autorii Ryuk s-au dovedit a fi același grup, care a devenit faimos pentru furtul codului lor simultan cu ransomware-ul Hermes. Utilizarea algoritmilor militari și atacurile țintite asupra companiilor mari sunt principalele caracteristici ale Ryuk. În plus, majoritatea victimelor sale au fost obligate să plătească răscumpărarea Bitcoin.

DHARMA este un virus cripto care a apărut pentru prima dată în 2016. Mai multe versiuni sunt încă lansate. În plus față de criptarea fișierelor victimei, Dharma șterge orice copie-umbră. În 2019, s-a răspândit prin contaminarea fișierelor cu extensii populare, dăunătoare sau legitime, cum ar fi ,,gif, ,,AUF", ,,USA", ,,xwx", ,,best" și ,,heets". Pentru a ajuta victimele Dharma să-și decripteze fișierele, un cercetător de securitate a lansat Rakhnidecryptor42 în septembrie 2019.

GANDCRAB, care a fost utilizat pentru prima dată în ianuarie 2018, a infectat peste 50 000 de sisteme în mai puțin de o lună, devenind unul dintre cele mai populare programe ransomware din 2018. Pentru an ataca fără a fi detectat, folosește macrocomenzile Microsoft Office, VBScript și PowerShell. GandCrab și Cerber folosesc modelul ransomware-as-a-service sau RaaS, care permite dezvoltatorilor și infractorilor să împărtășească profiturile. După ce a piratat serverele GandCrab, o echipă formată din Europol, Poliția Română, Procuratura Generală și Bitdefender a dezvoltat un instrument de decriptare. După ce au primit plăți de răscumpărare de peste 2 miliarde de dolari americani, operatorul GandCrab și-a anunțat retragerea în trimestrul doi al anului 2019. Cu toate acestea, ransomware-ul Sodinokibi, care este observat sporadic, este considerat a fi succesorul lui GandCrab.

În iunie 2019, REVIL (cunoscut și sub numele de SODINOKIBI sau SODIN_) a apărut pentru prima dată într-un atac web asupra instrumentului WinRAR din Italia. În plus, este acuzat de implicare în trei atacuri MSP și încă unul împotriva companiei americane PerCSoft, a cărei clientelă provine în principal din domeniul medical. Sodinokibi pare a fi un produs al FruityArmor, un grup de spionaj cibernetic renumit care funcționează din 2016. Sodinokibi au avut un impact în multe țări din întreaga lume. Taiwan este națiunea cea mai afectată de atacurile Sodinokibi, deoarece a suferit până în prezent 17,56 % din toate atacurile raportate. Germania (8,05 %), Italia (5,12 %) și Spania (4,88 %) sunt cele mai vizate țări din Europa. Sodinokibi funcționează printr-un model RaaS și criptează fișierele care sunt necesare pentru un atac per-sistem. Utilizarea unei „chei schelet" în codul atacatorilor le permite să decripteze fișierele de la distanță, indiferent de criptarea originală. Cu toate acestea, Sodinokibi nu poate cripta un computer cu o tastatură rusească, armeană, siriană sau oricare altceva. Acest lucru indică probabil originea autorilor.

Pentru al cincilea a consecutiv, SAMSAM se concentrează pe infrastructura vitală din întreaga lume. Spitalele, companiile medicale și organizațiile guvernamentale sunt ținta principală a atacurilor SamSam pentru a garanta plata rapidă a răscumpărărilor mari. Utilizează vulnerabilitățile RDP. Grupul care se ocupă de distribuirea SamSam a adunat până acum peste 6 milioane USD[44] (aproximativ 5 milioane EUR[45]) în plăți de răscumpărare și a plătit peste 30 de milioane USD (aproximativ 25,4 milioane EUR) victimelor. Costurile pentru reparații și daune s-au ridicat la 17 milioane USD (aproximativ 14,4 milioane EUR) doar în urma atacului din 2018 asupra orașului Atlanta.

[44] USD- dolari americani;
[45] EUR-euro;

Atacurile de tip ransomware vizează anumite sectoare ce sunt ofertante pentru răfăcătorii cibernetici. Principalele sectoare afectate de atacurile cibernetice de tip ransomware sunt organizațiile statelor și instituțiile publice ale națiunilor, instituțiile de învățământ, sectorul sănătății și cel al furnizorilor de servicii.

Statele-națiune sunt într-un real pericol încă de la apariția criminalității cibernetice, în special atunci când ransomware-ul este folosit pentru a viza organizații ale statelor-națiune ca mijloc de a obține bani. În 2019, națiunile sau grupurile naționale și-au deghizat identitatea folosind aceleași instrumente create de alte grupuri sau actorii statului-națiune. Această manipulare a instrumentelor permite atacatorului să rămână anonim și să-și protejeze țara de represalii diplomatice, în special în cazul în care ținta este o organizație guvernamentală sau de stat. Tot în anul 2019, au avut loc mai multe atacuri împotriva instituțiilor guvernamentale sau de stat. Unul dintre aceste atacuri a cerut conducerii orașului Lodi din California să plătească 400 000 USD, sau aproximativ 340 000 EUR, ca răscumpărare pentru a debloca liniile telefonice ale poliției, liniile de urgență ale departamentului de lucrări publice, numerele primăriei și sistemele financiare și de date de plată ale orașului. Orașul a refuzat să se conformeze și și-a recuperat datele folosind copii suplimentare pentru a opri atacul. Departamentul de resurse informaționale din Texas a raportat un atac ransomware planificat asupra a 23 de mici organizații guvernamentale în august 2019. Se estimează că pagubele din statul Texas au fost estimate la aproximativ 3,25 milioane USD (sau 2,75 milioane EUR). Un atac RobbinHood a avut loc în Baltimore și a cauzat o pierdere de 18,2 milioane USD (aproximativ 15,4 milioane EUR), în timp ce un atac Ryuk an avut loc în Lake City, Florida, și a cauzat o pierdere de 460 000 USD (aproximativ 389 768 EUR). Orașul New Bedford din Massachusetts a fost, de asemenea, victima unui atac de răscumpărare în iulie 2019. I s-a cerut să plătească 5,3 milioane USD (aproximativ 4,4 milioane EUR) pentru răscumpărare. Orașul a refuzat să plătească răscumpărarea și a cheltuit în schimb un milion de dolari pentru a-și îmbunătăți situația de securitate după atac.

Instituțiile de învățământ se alătură listei victimelor atacurilor de tip ransomware: atacurile s-au concentrat mai mult pe instituțiile de învățământ în 2019 față de anul precedent. Un raport publicat de compania de securitate Emsisoft spune că 62 de incidente ransomware au afectat 1051 de școli și instituții de învățământ. În 2018, doar șaisprezece incidente au avut loc în instituțiile de învățământ. Conform raportului, școlile din Statele Unite au fost a doua cea mai frecventă categorie de victime, după municipalitățile locale.

Sectorul sănătății continuă să sufere din cauza atacurilor ransomware. În anii trecuți, organizațiile medicale au fost ținta preferată a atacatorilor ransomware, iar această tendință persistă și în prezent. Furnizorul de servicii medicale Wood Ranch Medical din California a fost ținta unui atac în timpul verii anului 2019. Refuzul lor de a plăti răscumpărările a dus la distrugerea fișelor medicale electronice ale companiei, inclusiv copiile de rezervă. Prin urmare an incidentului, Wood Ranch Medical a trebuit să anunțe că își va sista activitatea până la sfârșitul anului. Un alt furnizor de servicii medicale, Centrul Brookside ENT and Hearing din Michigan, a fost nevoit să înceteze în aprilie 2019 din cauza aceleiași serii de evenimente. În plus, două grupuri de spitale din Australia, GippslandHealth Alliance și South West Alliance of Rural Health, au fost atacate. Deoarece sistemele lor au fost deconectate pentru a reduce expunerea pacienților, spitalele din mai multe orașe, cum ar fi Warrnambool, Colac, Geelong, Warragul, Sale și Bairnsdale, nu au putut oferi pacienților tratamentele și procedurile normale. Pierderea de date în acest sector este la fel de dăunătoare ca pierderea de bani. De exemplu, un atac ransomware care a vizat grupul Premier Family Medical din Utah în iunie 2019 a dezvăluit informațiile protejate privind sănătatea a peste 300 000 de pacienți.

Multe sectoare de afaceri se bazează pe furnizorii de servicii gestionate (MSP) și furnizorii de servicii cloud (CSP) pentru păstrarea datelor sensibile vitale pentru funcționarea lor. În plus, acestea se bazează pe astfel de furnizori pentru a se asigura că datele lor sunt sigure și că nimeni nu poate avea acces neautorizat la ele. Cu toate acestea, programele ransomware GandCrab și Sodin folosesc vulnerabilitățile MSP-urilor pentru a expune infrastructura și datele lor,

permițând atacurilor ransomware să afecteze întreaga clientelă MSP. Aceste vulnerabilități sunt incluse în instrumentul MSP comun Webroot2FA, care a fost folosit în mai multe cazuri în 2019. [36]

2.4. Vulnerabilitățile sistemelor în fața atacurilor cibernetice

Amenințările din lumea virtuală sunt caracterizate printr-o asimetrie accentuată și o dinamică globală. Acest lucru le face dificil de identificat și de contracarat prin măsuri proporționale cu efectele materializării riscurilor. Având în vedere interdependența din ce în ce mai mare între infrastructurile cibernetice și infrastructurile din domeniile financiar-bancar, transport, energie și apărare națională, spațiul informatic se confruntă în prezent cu amenințări cibernetice la adresa infrastructurilor critice. Deoarece lumea virtuală este atât de extinsă, atât sectorul privat, cât și cel public sunt expuse riscurilor crescute.

Deși există numeroase categorii de amenințări cibernetice bazate pe motivație și impactul lor asupra societății, cea mai răspândită este cea care se bazează pe internet. În acest sens, putem lua în considerare infracțiunile cibernetice, terorismul cibernetic și războiul cibernetic, care au ca sursă atât entități guvernamentale, cât și non-guvernamentale.

În cele mai multe cazuri, amenințările din mediul online se materializează prin utilizarea vulnerabilităților care provin din natura umană, tehnică și procedurală precum:

- atacuri cibernetice care afectează infrastructuri care susțin funcții de utilitate publică sau servicii ale societății informaționale care pot pune în pericol securitatea națională;
- accesul în mod neautorizat în infrastructura cibernetică;
- modificarea, ștergerea sau deteriorarea neautorizată a datelor informatice sau limitarea ilegală an accesului la aceste date;
- spionajul cibernetic;

Principalele amenințări la adresa spațiului cibernetic provin de la mai mulți posibili actori. Prima categorie de actori este cea a persoanelor sau grupurilor criminale organizate care exploatează vulnerabilitățile spațiului cibernetic pentru a obține beneficii patrimoniale sau nepatrimoniale. Cea de-a doua categorie este reprezentată de actorii responsabili pentru planificarea și coordonarea atacurilor teroriste sau extremiste ce au loc în mediul public digital. Scopurile acestor actori sunt de a realiza activități de comunicare, propagandă, colectare de fonduri, de recrutare și instruire în vederea creșterii numărului de adepți dar și pentru alte scopuri rău intenționate. Ultima categorie de actori ce reprezintă o amenințare la adresa spațiului cibernetic sunt statele sau organizațiile non-statale care încep sau desfășoară operațiuni în spațiul cibernetic cu scopul de a colecta informații din domeniile guvernamentale, militare, economice sau pentru a prezenta alte amenințări la securitatea națiunii. [37]

Agenția Uniunii Europene pentru Securitate Cibernetică evidențiază existența a opt categorii de vulnerabilități ale sistemelor. Această listă a fost realizată ca urmare a numărului, gradului de pericol și atractivitatea pe care aceste vulnerabilități au căpătat-o în fața răufăcătorilor cibernetici. Cele opt categorii sunt: ransomware, malware, ingineria socială, amenințările la adresa datelor, amenințările provenite de la atacuri de tip DdoS, amenințări provenite de pe internet, dezinformarea sau informarea greșită și atacurile de tip Supply Chain.

Ransomware-ul este descris ca un fel de atac atunci când actorii amenințărilor preiau controlul asupra activelor unei ținte și cer o răscumpărare în schimbul disponibilității activului, conform studiului ENISA ,,Threat Landscape for Ransomware Attacks". Această abordare independentă de acțiune este necesară pentru a ține cont de evoluția mediului de amenințări ransomware, de prezența mai multor strategii de extorcare și de obiectivele variate ale infractorilor care depășesc simplul câștig financiar. În perioada de raportare, ransomware-ul a fost din nou una dintre cele mai importante amenințări, cu numeroase cazuri importante și bine documentate.

Malware este un cuvânt umbrelă folosit pentru a descrie orice program sau firmware destinat să efectueze o procedură neautorizată care ar afecta negativ confidențialitatea, integritatea sau

disponibilitatea unui sistem. Este denumit și cod rău intenționat sau logică dăunătoare. Virușii, viermii, caii troieni și alte entități care infectează o gazdă sunt exemple de programare rău intenționată din trecut. Codul rău intenționat include, de asemenea, spyware și diferite tipuri de adware. Instanțele care au fost examinate de raportul ENISA au implicat în primul rând națiuni UE.

Termenul de „inginerie socială" se referă la o mare varietate de operațiuni care urmăresc să profite de un eșec sau de un comportament uman pentru a obține acces la date sau servicii. Folosește o varietate de tehnici de manipulare pentru a înșela oamenii să facă erori sau să dezvăluie informații private sau sensibile. Ingineria socială în securitatea cibernetică atrage oamenii să deschidă documente, fișiere sau e-mailuri, să viziteze site-uri web sau să ofere utilizatorilor neautorizați acces la sisteme sau servicii. Și chiar dacă aceste tactici pot folosi greșit tehnologia, ele depind întotdeauna de o componentă umană pentru a funcționa. Această pânză de amenințări cuprinde în primul rând următorii vectori, care sunt examinați în capitolul respectiv: phishing, spearphishing, smishing, vishing, compromis de e-mail de afaceri (BEC), fraudă, uzurparea identității și contrafacerea.

Amenințările la adresa datelor sunt un grup de amenințări care sunt direcționate către sursele de date cu intenția de a obține acces neautorizat, de a dezvălui date și de a modifica datele pentru a afecta comportamentul sistemului. Multe alte pericole, care sunt incluse și raportul realizat de ENISA, se bazează pe aceste riscuri. De exemplu, ransomware, RDoS (Ransomware Denial of Service) și DDoS (Distributed Denial of Service) încearcă să împiedice accesul la date și pot cere plata pentru a permite accesul să fie restabilit. Amenințările la adresa datelor se încadrează din punct de vedere tehnic în două categorii: încălcarea datelor și scurgerea datelor. O încălcare a datelor este un atac lansat intenționat de un infractor cibernetic cu scopul de a obține acces neautorizat și de a dezvălui date private sau protejate. Scurgerile de date pot avea loc din mai multe motive, inclusiv din cauza setărilor incorecte, defectelor de securitate sau greșelilor umane și au ca rezultat expunerea accidentală a datelor sensibile, confidențiale sau protejate.

O mare varietate de amenințări și atacuri, inclusiv DDoS, țintesc disponibilitatea sistemelor. Deși nu este o amenințare nouă, DDoS vizează disponibilitatea sistemelor și a datelor și joacă un rol important în peisajul amenințărilor de securitate cibernetică. Când utilizatorii unui sistem sau serviciu nu pot accesa date, servicii sau alte resurse relevante, înseamnă că a avut loc un atac. Acest lucru poate fi realizat prin suprasolicitarea resurselor serviciului sau a părților componente ale infrastructurii de rețea. Riscurile la adresa disponibilității și ransomware-ul sunt cele mai importante riscuri în timpul perioadei de raportare, ceea ce reprezintă o schimbare față de raportul precedent din 2021, când ransomware-ul se afla în mod incontestabil în top.

Viața tuturor este afectată de utilizarea internetului și de fluxul liber al informațiilor. Pentru multe persoane, accesul la internet a devenit o cerință de bază pentru a-și face meseria, munca școlară, pentru a-și exercita drepturile politice și sociale și pentru a interacționa cu ceilalți. Acest grup abordează pericole precum deturnarea BGP (Border Gateway Protocol) care afectează disponibilitatea internetului. Datorită influenței sale unice asupra mediului de amenințare, refuzul serviciului (DoS) este tratat într-o secțiune distinctă.

Campaniile de răspândire a informațiilor false și a dezinformarii sunt încă în creștere, datorită utilizării tot mai mari a rețelelor sociale și a sericiilor media online. În știrile și media de astăzi, canalele digitale sunt standardul. Astăzi, o mulțime de persoane folosesc site-urile de rețele sociale, canalele de știri și media și chiar motoarele de căutare ca surse de informații. Din cauza modului în care aceste site-uri web câștigă bani prin ademenirea vizitatorilor către site-urile lor, iar conținutul care atrage cei mai mulți spectatori este adesea utilizat fără a fi verificat. Conflictul dintre Rusia și Ucraina a demonstrat metode noi de a folosi această amenințare, urmărind să influențeze percepția oamenilor despre starea conflictului și rolurile jucate de părțile implicate. Distincția dintre informațiile inexacte și falsificarea intenționată este determinată de o varietate de factori. În această situație se aplică definițiile dezinformarii și al informării false.

Un atac asupra supply chain (lanțul de aprovizionare) se concentrează pe parteneriatul dintre întreprinderi și furnizorii săi. În sensul acestui raport, uitându-ne la criteriile găsite în ,,Threat Landscape for Ransomware Attacks" realizat de ENISA pentru supply chain care afirmă că un atac are o componentă a supply chain dacă combină cel puțin alte două atacuri. Un atac de tip supply chain trebuie să vizeze atât furnizorul, cât și clientul pentru a se califica în această categorie. Unul dintre cele mai vechi exemple ale acestui tip de asalt a fost SolarWinds, care a demonstrat, de asemenea, posibilele consecințe ale grevelor lanțului de aprovizionare. [38]

Capitolul 3. Studiu de caz- Atacurile cibernetice de tip Ransomware în mediul public digital

În ultimul capitol al acestei lucrări am decis să analizez un atac de tip ransomware ce a avut loc în mediul public digital. Cazul ales pentru acest studiu de caz este cel al atacului ransomware intitulat ,,WannaCry". Totul începe în luna mai a anului 2017 când WannaCry a început să se răspândească în întreaga lume infectând calculatoarele ce rulau sistemul de operare Windows. Principalul vinovat pentru răspândirea atât de rapidă a acestui ransomware a fost faptul că foarte mulți din utilizatorii de dispozitive ce foloseau sistemul de operare Windows nu își actualizau sistemul. Cu aproximativ 2 luni înainte, compania Microsoft (cea care a dezvoltat sistemul de operare Windows) a realizat o actualizare de securitate a sistemului ce avea ca țintă EternalBlue[46], o unealtă folosită de Windows pentru a implementa serviciul SMB[47]. Atacatorii s-au folosit de această unealtă pentru a infecta dispozitivele neactualizate ce nu beneficiau de protecția oferită de ultima actualizare oferită de compania Microsoft. Astfel, acești utilizatori au fost vulnerabili în fața atacului la scară largă WannaCry.

Atacatorii din spatele WannaCry au reușit astfel să cripteze calculatoarele a peste 230.000 de utilizatori din 150 de țări în doar câteva ore. Pentru a beneficia de o cheie de decriptare, victimele erau puse să plătească o răscumpărare de 300 de dolari americani (mai târziu această sumă a crescut la 600 de dolari americani) sub forma criptomonedei Bitcoin. Această metodă de încasare a răscumpărării este cea mai folosită metodă de plată solicitată de către atacatori datorită modului în care suma este transferată de la victime la atacatori (prin intermediul unei rețele aceste criptomonede ,,își pot pierde" foarte ușor urma, atacatorii profitând de această caracteristică pentru a nu fi interceptați de poliție). Atacul ransomware WannaCry și-a avertizat victimele că fișierele lor vor fi șterse ireversibil dacă nu plătesc răscumpărarea în trei zile. Mesajul afișat de atacatori poate fi văzut în figura 21.

Fig. 21 Mesajul afișat victimelor WannaCry
Sursa: https://www.healthcareitnews.com/news/wannacry-timeline-how-it-happened-and-industry-response-ransomware-attack

[46] EternalBlue- reprezintă unul dintre puținele „instrumente de exploatare" puse la dispoziție de un grup cunoscut sub numele de The Shadow Brokers (TSB) care exploatează vulnerabilități în modul în care Windows a implementat protocolul Server Message Block (SMB) se numește EternalBlue. Această vulnerabilitate a fost exploatată de tulpinile de ransomware WannaCry și NotPetya pentru a ataca computerele vulnerabile.
[47] SMB- acronim pentru Server Message Block sau tradus în limba română „Blocul de mesaje server"

WannaCry și alte programe ransomware funcționează în general prin blocarea dispozitivului sau criptarea fișierelor ce sunt stocate pe acesta și cererea unei răscumpărări pentru a oferi victimelor o cheie de decriptare. În cele mai multe cazuri suma cerută drept răscumpărare este solicitată sub formă de criptomonede, cea mai utilizată dintre acestea fiind Bitcoin. Apoi, deoarece aceste criptomonede sunt mai greu de urmărit decât transferurile electronice, cecurile sau numerarul real, solicită plata sub forma unei criptomonede precum Bitcoin. [39] Oamenii au crezut mai întâi că atacul ransomware WannaCry a fost distribuit printr-un atac de tip phishing, adică atunci când e-mailurile spam sunt folosite pentru a păcăli utilizatorii să descarce malware prin includerea de link-uri sau fișiere infectate. „Ușa din spate" plasată pe dispozitivele infectate (folosite pentru a rula WannaCry) a fost DoublePulsar, în timp ce EternalBlue a fost unealta care a permis WannaCry să se răspândească. [40] Cu toate acestea, în comparație cu atacurile clasice ransomware WannaCry diferă în câteva moduri. Pentru atacurile țintite, criminalii cibernetici folosesc adesea tulpini clasice de ransomware. Ca o analogie, considerați aceste atacuri mai mult ca un arc cu săgeți decât ca pe o catapultă. Primul este superior pentru aplicațiile cu o singură țintă, în timp ce cel de-al doilea este superior pentru aplicațiile cu mai multe ținte. De exemplu, software-ul și organizația criminală responsabile pentru atacul ransomware Colonial Pipeline păreau să aibă o singură țintă în minte. Se pare că grupul a folosit o parolă binecunoscută pentru un cont de rețea privată virtuală(VPN) mai vechi pentru a răspândi malware-ul DarkSide. Cu toate acestea, WannaCry a fost mai mult ca o catapultă. A infectat rapid zeci de mii de dispozitive din peste 150 de țări. A atacat rapid tot felul de sisteme prin intermediul rețelelor comerciale, fără a lua prizonieri. Așadar, factorii ce au dus la răspândirea atât de rapidă a ransomware-ului WannaCry la sacră atât de largă într-un timp atât de scurt au fost:

- Componenta de vierme informatică a acestuia- așa cum am explicat și în capitolul anterior, un vierme este o formă de malware care se poate propaga rapid fără un fișier gazdă, distruge datele și consumă lățimea de bandă. Se autopropagă, prin urmare, spre deosebire de virus, își poate începe acțiunea dăunătoare fără implicarea umană. Viermii pot răspândi și software rău intenționat, cum ar fi ransomware. Datorită viermelui care făcea parte din WannaCry, PC-urile Windowscare nu beneficiau de actualizarea de securitate au fost ținte sigure;
- Unealta SMB folosită de sistemul de operare Windows- un criminal cibernetic poate exploata o unealtă pentru a realiza un comportament distructiv asupra unei vulnerabilități a sistemului neactualizat. WannaCry a folosit o slăbiciune în modul în care Windows gestiona protocolul SMB (Server Message Block). Pe scurt, protocolul SMB permite comunicarea între nodurile de rețea. Deoarece mulți utilizatori Windows fie nu primesc actualizări ale sistemului fie nu le actualizează de bună-voie, criminalii cibernetici continuă să folosească vulnerabilitățile dispozitivelor neactualizate chiar și după ce aceste informații au fost făcute publice.

Datorită vitezei mari cu care WannaCry s-a răspândit, un număr mare de sectoare a fost afectat de acest atac cibernetic. Printre cele mai importante sectoare afectate au fost:

- Sectorul sănătății;
- Sectorul urgențelor;
- Sectorul securității;
- Sectorul logistic;
- Sectorul de telecomunicații;
- Industria petrolieră;
- Sectorul automatizărilor;
- Sectorul educației;
- Sectorul ce se ocupă de publicitate.

Astfel, infectând cele aproximativ 230.000 de dispozitive, WannaCry a afectat activitatea spitalelor, serviciilor de urgență, a stațiilor de carburant și chiar activitatea mai multor fabrici și linii de producție. Potrivit unor estimări atacul a provocat daune de ordinul miliardelor de dolari americani.

Atacul WannaCry este atribuit oficial Coreei de Nord de către SUA, iar trei nord-coreeni au fost chiar acuzați că sunt responsabili atât pentru WannaCry, cât și pentru un alt atac asupra Sony Pictures Entertainment în anul 2014. Este interesant de observat că, în mod neintenționat, NSA (Agenția Națională de Securitate) ar fi putut contribui la atacul WannaCry. Potrivit zvonurilor, Agenția Națională de Securitate (NSA) a descoperit defectul SMB de care se folosește WannaCry. Mai târziu, se spune că un grup de hackeri numit The Shadow Brokers (TSB) a achiziționat așa-numitul instrument de exploatare EternalBlue de la o agenție de spionaj și l-a lansat online.

În cazul atacurilor de tip ransomware precum WannaCry, când vine vorba de plata răscumpărărilor, sugestia este să nu se cedeze în fața presiunii puse de atacatori. Este indicat ca plata răscumpărării să nu fie niciodată făcută, deoarece nu există nicio modalitate de a ști sigur dacă datele vor fi restaurate și în plus, fiecare plată efectuată îi susține pe atacatori, crescând probabilitatea unor noi atacuri pe viitor. Această recomandare a fost utilă în timpul atacului WannaCry, deoarece, potrivit rapoartelor, codul atacului era viciat. Atacatorii nu au reușit să conecteze plățile de răscumpărare făcute de victime la computerul lor, nereușind astfel să intre în posesia sumelor de bani cerute. Există un scepticism substanțial cu privire la cine a primit informațiile returnate. Unii oameni de știință au spus că nimeni nu a primit niciodată datele înapoi. Cu toate acestea, F-Secure, o afacere din domeniul securității cibernetice, a spus că unele victime au făcut-o. Acest lucru este o dovadă clară a faptului că, în cazul unui atac ransomware, plata răscumpărării nu este niciodată o idee inteligentă.

Operatorul spaniol de telefoane mobile Telefónica a fost una dintre primele afaceri afectate. Până pe 12 mai, sute de clinici și spitale NHS[48] din Regatul Unit au fost afectate. Trusturile de spitale atacate din NHS reprezentau o treime din ținte. Se pare că ambulanțele au fost deviate într-un mod inadecvat, lăsând pacienții ce aveau nevoie de tratament de urgență să aștepte un timp îndelungat. După ce 19.000 de întâlniri au fost amânate din cauza incidentului, s-a calculat că va costa NHS 92 de milioane de lire sterline.

Pentru a evita alte atacuri de acest tip, specialiștii în securitatea cibernetică recomandă utilizatorilor să manifeste precauție în ceea ce rivește datele stocate și utilizarea acestora în mediul public digital dar și să urmeze următoarele indicații:

- Să își actualizeze în mod regulat softwear-ul și sistemul de operare al dispozitivului;
- Să nu acceseze link-uri suspecte;
- Să nu deschidă atașamentele din e-mailuri provenite din surse necunoscute;
- Să nu descarce conținut de pe site-uri care nu par a fi legitime;
- Să evite introducerea de dispozitive USB necunoscute;
- Să folosească un serviciu VPN atunci când utilizează rețele Wi-Fi (rețele wireless);
- Să folosească un software de securitate certificat pentru navigarea pe internet;
- Să actualizeze constant software-ul de securitate al internetului;
- Să își realizeze copii de rezervă a tuturor datelor stocate pe dispozitive. [40]

O concluzie a acestui studiu de caz realizat pe baza atacului cibernetic WannaCry este aceea că oricât de inofensive ar putea părea, atacurile cibernetice sunt o reală amenințare la adresa securității spațiului public digital. În urma modelului analizat, putem constata că infractorii cibernetici se pot folosi de orice mică breșă de securitate a unui sistem pentru a profita de utilizatori, acest lucru ducând nu doar la pierderi financiare ci și la amenințarea vieții persoanelor nevinovate, cum s-a putut observa în cazul WannaCry asupra sistemului de sănătate și al serviciilor de urgență.

[48] NHS- abreviere pentru National Health Service reprezintă Serviciul Național de Sănătate al Marii Britanii

Bibliografie

[1] Z. Aureliu, "Criptarea și securitatea informației," Chișinău, 2013.

[2] "Open Vision," [Online]. Available: https://www.openvision.ro/blog/academia-it/ce-este-criptografia-cum-algoritmii-pastreaza-informatiile-secrete-si-sigure/. [Accessed 04 04 2023].

[3] G. M. Zoran Constantinescu, Criptarea Informației- Ghid practic, Ploiești, România: Editura Universității Petrol-Gaze din Ploiești, 2013.

[4] R. Churchhouse, Codes and ciphers- Julius Caesar, the Enigma, and the internet, Cambridge: The press syndicate of the University of Cambridge, 2002.

[5] L. D. Smith, „Substitution Ciphers". Cryptography the Science of Secret Writing: The Science of Secret Writing., Dover Publications, 1943.

[6] I. Popovici, "Criptografia, metoda pentru asigurarea securității tranzacțiilor de date," in *Analele Științifice ale Universității de Stat ,,B.P.Hașdeu"*, Cahul, 2012.

[7] A. Pătrușcă, "Evenimentul Istoric," 27 06 2021. [Online]. Available: https://evenimentulistoric.ro/matematicianul-de-geniu-care-a-spart-enigma.html. [Accessed 07 04 2023].

[8] B. Groza, Introducere în Criptografie, Funcții Criptografice, Fundamente Matematice și Computaționale, Timișoara, 2012.

[9] I. d. F. M. Conf. dr. ing. Luminița Scripcariu, "Revista Intelligence," 2 05 2019. [Online]. Available: https://intelligence.sri.ro/tehnici-de-criptare-tendinte-actuale-securitatea-informatiei/. [Accessed 07 04 2023].

[10] "Securitatea Informațiilor," 07 05 2013. [Online]. Available: https://www.securitatea-informatiilor.ro/solutii-de-securitate-informatica/algoritmul-de-criptografie-rsa/. [Accessed 07 04 2023].

[11] d. I. Gogota, "Biblioteca Județeană Petre Dulfu- Baia Mare," 06 04 2021. [Online]. Available: https://www.bibliotecamm.ro/bibliotheca-septentrionalis/protectia-datelor-personale-si-mediul-online/2021/04/06/. [Accessed 27 05 2023].

[12] A. Stroe, "Business Magazin," 28 01 2020. [Online]. Available: https://www.businessmagazin.ro/actualitate/cum-ne-putem-proteja-datele-personale-in-mediul-online-18758908. [Accessed 18 05 2023].

[13] Cisco, "What is Cybersecurity?," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. [Accessed 29 04 2023].

[14] Q. L. Yuchong Li, "A comprehensive review study of cyber-attacks and cyber security;," *Elsevier,* 2021.

[15] C. Griffiths, "The latest 2023 Cyber Crime Statistics," AAG, 06 04 2023. [Online]. Available: https://aag-it.com/the-latest-cyber-crime-statistics/. [Accessed 29 04 2023].

[16] A. Wolf, "A Brief History of Cybercrime," 16 11 2022. [Online]. Available: https://arcticwolf.com/resources/blog/decade-of-cybercrime/. [Accessed 29 04 2023].

[17] C. Hope, "Punch Card," 05 02 2021. [Online]. Available: https://www.computerhope.com/jargon/p/punccard.htm. [Accessed 29 04 2023].

[18] FBI, "The Morris Worm- 30 Years Since First Major Attack on the Internet," 02 11 2018. [Online]. Available: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218. [Accessed 29 04 2023].

[19] WOWHOST, "Biblioteca de cunoștințe," WowHost, [Online]. Available: https://www.wowhost.ro/clienti/knowledgebase/388/Ce-este-un-virus-informatic-Clasificarea-virusilor-informatici-....html. [Accessed 10 05 2023].

[20] FBI, "The Melissa Virus- An 80$ Milion Cyber Crime in 1999 Foreshadowed Modern Threats," 25 03 2019. [Online]. Available: https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519. [Accessed 06 05 2023].

[21] Trellix, "Trellix," [Online]. Available: https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html#definition. [Accessed 26 05 2023].

[22] Crowdstrike, "The Zeus trojan malware- definition and prevention," 14 03 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware/. [Accessed 28 05 2023].

[23] D. V. F. Popescu, "Vulnerabilități și amenințări din spațiul cibernetic vs. arhitectura de securitate la diferite niveluri," *Conferința științifică internațională gândirea militară românească.*

[24] Microsoft, "Ce este un atac cibernetic?," [Online]. Available: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack. [Accessed 28 05 2023].

[25] NordVPN, "Ce este malware-ul?," [Online]. Available: https://nordvpn.com/ro/cybersecurity/what-is-malware/. [Accessed 28 05 2023].

[26] Bitdefender, "Cum eliminați Adware-ul, ferestrele pop-up și redirecționările în browser pe Windows," Bitdefender, [Online]. Available: https://www.bitdefender.ro/consumer/support/answer/21720/. [Accessed 28 05 2023].

[27] ESET, "Spyware," ESET, [Online]. Available: https://help.eset.com/glossary/ro-RO/spyware.html. [Accessed 28 05 2023].

[28] Bitdefender, "Ce este Spyware-ul? Prevenire și eliminare," Bitdefender, [Online]. Available: https://www.bitdefender.ro/consumer/support/answer/83301/. [Accessed 28 05 2023].

[29] MacroTehnicus, "Totul despre viruși informatici," [Online]. Available: https://macrotehnicus.ro/totul-despre-virusi-informatici/. [Accessed 28 05 2023].

[30] Wowhost, "Ce este un virus informatic? Clasificarea virusilor informatici," Wowhost, [Online]. Available: https://www.wowhost.ro/clienti/knowledgebase/388/Ce-este-un-virus-informatic-Clasificarea-virusilor-informatici-....html. [Accessed 28 05 2023].

[31] PCLaptop, "Viermii informatici," 23 05 2015. [Online]. Available: https://pclaptop.ro/viermii-informatici/. [Accessed 28 05 2023].

[32] Malwarebytes, "Worm," Malwerbytes, [Online]. Available: https://www.malwarebytes.com/blog/threats/worm. [Accessed 29 05 2023].

[33] Bitdefender, "Ce este un Troian? Prevenire și Eliminare," Bitdefender, [Online]. Available: https://www.bitdefender.ro/consumer/support/answer/76459/. [Accessed 29 05 2023].

[34] K. Glamoslija, "Ce este un Cal Troian și Cum să Vă Protejați Împotriva Acestuia," SafetyDetectives, [Online]. Available: https://ro.safetydetectives.com/blog/ce-este-un-cal-troian-si-cum-sa-va-protejati-impotriva-acestuia/. [Accessed 29 05 2023].

[35] DepanareLaptop.ro, "Ransomware – Ce este, cum se manifesta si cum se pot evita neplacerile cauzate de acesta?," [Online]. Available: https://www.depanarelaptop.ro/Articole/noutati-laptop/ransomware-ce-este-cum-se-manifesta-si-cum-se-pot-evita-neplacerile-cauzate-de-acesta/. [Accessed 30 05 2023].

[36] ENISA, "Ransomware (programele de șantaj digital)," European Union Agency for Cybersecurity, 2020.

[37] ENISA, "Strategia de securitate cibernetică a României," [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf. [Accessed 30 05 2023].

[38] ENISA, "ENISA Threat Landscape 2022," 2022.

[39] Malwarebytes, "WannaCry," [Online]. Available: https://www.malwarebytes.com/wannacry. [Accessed 30 05 2023].

[40] Kaspersky, "What is WannaCry ransomware?," [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. [Accessed 30 05 2023].

[41] C. Neagu, "Digital Citizen," 15 05 2023. [Online]. Available: https://www.digitalcitizen.ro/intrebari-simple-este-usb-sau-magistrala-seriala-universala/. [Accessed 27 05 2023].

[42] Malwarebytes, "Keylogger and keystroke logger spyware," [Online]. Available: https://www.malwarebytes.com/keylogger. [Accessed 27 05 2023].

[43] "Dex Online," [Online]. Available: https://dexonline.ro/definitie/hacker. [Accessed 28 05 2023].

[44] NordVPN, "Stalkerware," [Online]. Available: https://nordvpn.com/ro/cybersecurity/glossary/stalkerware/. [Accessed 28 05 2023].

[45] ITUSER, "GPT sau MBR? Cum afli ce disc ai la calculator?," 13 10 2018. [Online]. Available: https://ituser.info/windows/gpt-sau-mbr-cum-afli-ce-disc-ai-la-calculator-ce-este-gpt. [Accessed 28 05 2023].

[46] T. Fisher, "Ce este un sector de boot?," eYewated, [Online]. Available: https://ro.eyewated.com/ce-este-un-sector-de-boot/. [Accessed 29 05 2023].

[47] Codecool, "Ghidul începătorului în Java," 2023 01 30. [Online]. Available: https://codecool.com/ro/blog/ghid-java-incepatori/. [Accessed 29 05 2023].

[48] D. Grigori, "Ce însemnă ROOT pe telefoane Android - noțiune și avantaje," 09 01 2020. [Online]. Available: https://www.grigdroid.ro/2016/06/tot-ce-trebuie-sa-stii-despre-root.html. [Accessed 29 05 2023].

[49] Malwarebytes, "WannaCry," [Online]. Available: https://www.malwarebytes.com/wannacry. [Accessed 30 05 2023].

[50] Banca Națională a României, "Centrala Incidentelor de Plăți," [Online]. Available: https://www.bnr.ro/Centrala-Incidentelor-de-Plati-(CIP)-718-Mobile.aspx. [Accessed 28 04 2023].