3. PROGRAME MALWARE

Preliminarii

În această temă vor fi tratate subiecte care se referă la tipurile programelor malware, vor fi analizate comportamentele și elementele definitorii, care contribuie la detectarea și eradicarea programelor malițioase. Vor fi analizate modalitățile de prevenire a infectării cu programe malware.

Scopul:

- *studierea programelor malițioase, analiza comportamentelor și semnăturii specifice programelor malițioase comune.*

Obiectivele educaționale:

- *descrierea diferitor tipuri de malware și modul în care acestea funcționează;*
- *analiza diferențelor și asemănărilor dintre programele malware;*
- *identificarea și explicarea metodelor comune de răspândire a malware-ului;*
- *identificarea și descrierea măsurilor de protecție împotriva malware-ului.*

Finalitățile de referință:

- *cunoașterea programelor malware răspândite;*
- *capacitatea de a analiza și identifica în baza semnăturilor specifice programelor malițioase programul malițios;*
- *dezvoltarea abilităților de a efectua analiza statică și dinamică de bază a programelor malițioase;*
- *cunoașterea metodelor de protecție anti-malware.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs.

3.1. Programe malware

Software-ul rău intenționat, sau malware, este un termen folosit pentru a descrie software-ul conceput pentru a perturba operațiunile calculatorului sau pentru a obține acces la sistemele informatice, fără știrea sau permisiunea utilizatorului. Malware a devenit un termen umbrelă folosit pentru a descrie toate programele ostile sau intruzive. Termenul de malware include viruși de computer, viermi, cai troian, ransomware, spyware, adware, scareware, bombe logice, rootkit-uri, backdoor și alte programe rău intenționate [11]. Malware-ul poate fi evident și simplu de identificat, sau poate fi ascuns și aproape imposibil de detectat.

În continuare vor fi descrise cele mai răspândite programe malware.

Virus informatic

Un virus infectează calculatoarele fiind transmis prin e-mail, unități USB, transferuri de fișiere și chiar mesageria instantă. Virusul se ascunde, atașându-se de codul calculatorului, software-ul sau documentelor de pe calculator. Când fișierul este accesat, virusul execută și infectează calculatorul. Un virus care infectează fișierul de program executabil se numește *virus de program*. Când programul este lansat, virusul se activează. Un virus poate infecta și un fișier de date. Unul dintre cei mai comuni viruși de fișiere de date este un *virus macro*. O macrocomandă reprezintă o serie de instrucțiuni care pot fi grupate ca o singură comandă.

Adesea, macrocomenzile sunt folosite pentru a automatiza un set complex de sarcini sau o serie repetată de sarcini. Macro-urile pot fi scrise folosind un limbaj macro, cum ar fi Visual Basic pentru aplicații (VBA) și sunt stocate în documentul utilizatorului (cum ar fi ca într-o foaie de lucru Excel .XLSX sau fișier Word .DOCX) [12]. Odată ce documentul este deschis, se execută instrucțiunile macro. Un număr foarte mare de tipuri diferite de fișiere pot conține un virus. În tabelul 3.1 sunt descrise extensiile fișierelor care pot conține viruși în Windows.

Tabelul 3.1. Extensiile fișierelor ce pot fi infectate cu viruși informatici în Windows

Nr.	***Extensiile fișierelor***	***Descriere***
1.	.docx, .xlsx	Documente Microsoft Office
2.	.exe	Programe executabile
3.	.msi	Fișier de instalare Microsoft
4.	.msp	Fișierul patch de instalare Windows
5.	.scr	Windows screen saver
6.	.cpl	Fișierul Panoului de Control Windows
7.	.msc	Fișierul consolei de management Windows
8.	.wsf	Fișier script Windows
9.	.reg	Fișierul registrului din Windows
10.	.ps1	Fișierul PowerShell din Windows

De fiecare dată când programul infectat este lansat sau fișierul este deschis, fie de către utilizator, fie de către sistemul de operare al calculatorului, virusul efectuează două acțiuni. În primul rând, descarcă o sarcină utilă pentru a efectua o acțiune rău intenționată, apoi încearcă să se reproducă infectând alte fișiere. Deși virușii timpurii nu făceau adesea altceva decât să afișeze un mesaj enervant, virușii de astăzi sunt mult mai dăunători. Virușii pot efectua următoarele acțiuni:

- cauzează blocarea în mod repetat a unui calculator;
- ștergerea fișierelor de pe un hard disk;
- dezactivarea setărilor de securitate ale calculatorului;
- formatarea unităților de disc.

Virusul informatic se poate replica numai pe calculatorul- gazdă pe care se află; nu se poate răspândi automat la alt calculator de sine stătător.

Viermele informatic

Spre deosebire de virușii informatici care nu se pot reproduce independent pe alte calculatoare, viermii o pot face. *Un vierme este un program rău intenționat care utilizează o rețea de calculatoare pentru a se replica (viermii sunt uneori numiți viruși de rețea)*. Un vierme este proiectat să pătrundă într-un calculator prin rețea, apoi să profite de vulnerabilitatea unei aplicații sau a sistemului de operare pe calculatorul-gazdă. Când viermele a exploatat vulnerabilitatea pe un sistem, caută imediat un alt calculator din rețea care are aceeași vulnerabilitate. Viermii au provocat unele dintre cele mai răspândite atacuri pe Internet. De exemplu, în 2001, 658 de servere au fost infectate cu un vierme numit **Code Red**. După 19 ore, peste 300.000 de servere au fost infectate cu acest vierme informatic.

Calul troian

Un alt tip de malware este *calul troian.* Un *cal troian* arată de obicei ca un program util, însă conține un cod rău intenționat. De exemplu, *calul troian* este adesea furnizat cu jocurile gratuite online. Aceste jocuri sunt descărcate în calculatorul utilizatorului, dar conțin și un cod

malițios. În timpul jocului, *calul troian* este instalat pe sistemul utilizatorului și continuă să funcționeze chiar și după ce jocul a fost închis. Există mai multe tipuri de *cal troian*, după cum este descris în tabelul 3.2.

Tabelul 3.2. Tipuri de *cal troian*

Nr.	***Tip de cal troian***	***Descriere***
1	Acces de la distanță	Permite accesul neautorizat de la distanță
2	Trimitere date	Oferă atacatorului date cu caracter sensibil, ca de exemplu date de autentificare
3	Distructiv	Poate corupe sau șterge fișiere
4	Împuternicit	Va utiliza calculatorul infectat ca sursă pentru a lansa atacuri și pentru a efectua alte acțiuni ilegale
5	FTP	Permite servicii de transfer de fișiere neautorizate
6	Dezactivare software de securitate	Oprește antivirusul sau firewall-ul să funcționeze
7	DoS	Încetinește sau oprește activitatea rețelei

Rootkit

Unele tipuri de malware evită detectarea ca trăsătură principală, mascându-se. În această categorie pot fi atribuite rootkit-urile. Rootkit-urile se maschează schimbând sistemul de operare pentru a-l forța să ignore fișierele sau activitatea lor rău intenționată [11, 13]. De asemenea, rootkit-urile ascund sau elimină toate urmele de dovezi care pot dezvălui programele malware, cum ar fi intrările de jurnal. O abordare des utilizată de rootkit-uri este modificarea sau înlocuirea fișierelor sistemului de operare prin instalarea versiunilor noi, care sunt special concepute pentru a ignora dovezile rău intenționate. De exemplu, software-ul de securitate poate fi instruit să scaneze toate fișierele dintr-un anumit director. Pentru a face acest lucru, software-ul de scanare va primi o listă a acelor fișiere de la sistemul de operare. Un rootkit va înlocui lista exactă de fișiere a sistemului de operare cu propria rutină a rootkit-ului, care va face acest lucru fără a afișa fișierele rău intenționate.

3.2. Malware cu funcționalități specifice

Puterea distructivă a programelor malware se regăsește în capacitățile sale de încărcare utilă. Sarcina utilă principală este de a colecta date, de a șterge date, de a modifica setările de securitate ale sistemului și de a lansa atacuri. Sunt concepute diferite tipuri de programe malware pentru a colecta date importante de la calculatorul utilizatorului și a le pune la dispoziția atacatorului. Aceste malware includ *spyware, adware* și *ransomware*.

Spyware

Spyware este un termen general folosit pentru a descrie software-ul care spionează utilizatorii și colectează informații fără acordul lor (figura 3.1). Coaliția Anti-Spyware definește *spyware ca software de urmărire care este implementat fără notificare, consimțământ sau control adecvat din partea utilizatorului.*

Fig. 3.1. Exemplu de Spyware

Acest software folosește resursele calculatorului, inclusiv programele deja instalate pe calculator, în scopul colectării și distribuirii informațiilor personale sau sensibile. Se disting câteva tipuri de spyware:

- *software de descărcare automată* – utilizat pentru a descărca în mod automat software fără acțiuni din partea utilizatorului;
- *software de modificare a sistemului* – utilizat pentru a modifica configurările de sistem realizate de utilizator, așa ca pagina de start a browser-ului;
- *software de urmărire* – utilizat pentru a monitoriza activitatea utilizatorului sau pentru a colecta datele sensibile ale acestuia.

Nu toate programele spyware sunt malițioase, de exemplu, software-ul de monitorizare a activității copiilor permite părinților să gestioneze activitatea și durata de navigare a minorilor. Un tip de program similar este *keylogger-ul*, care înregistrează tastele acționate de utilizator și pot fi utilizate atât de angajatori pentru a monitoriza activitatea angajaților în timpul orelor de lucru, cât și de atacatori pentru a afla parolele sau alte informații sensibile.

Adware

Adware oferă conținut publicitar într-un mod neașteptat și nedorit de către utilizator (figura 3.2). Când malware-ul adware este instalat, acesta afișează de obicei bannere de publicitate, reclame pop-up, sau deschide noi ferestre de browser web la intervale aleatorii. Utilizatorii în general resping adware-ul deoarece:

- adware-ul poate afișa un conținut inacceptabil, cum ar fi site-uri de jocuri de noroc sau pornografie;
- anunțurile pop-up frecvente pot interfera cu productivitatea unui utilizator;
- anunțurile pop-up pot încetini un calculator sau chiar pot provoca blocări și pierderea de date.

Fig. 3.2 Exemplu de Adware

Ransomware

Unul dintre cele mai noi malware și cu cea mai rapidă răspândire este *ransomware*. Ransomware-ul împiedică funcționarea corectă a dispozitivului unui utilizator până când nu se achită o taxă ca în figura 3.3. Unele variante de ransomware blochează calculatorul unui utilizator, apoi afișează un mesaj care se pretinde provenind de la o agenție de stat, de exemplu. Acest mesaj folosește imagini cu aspect oficial, afirmă că utilizatorul a efectuat o acțiune ilegală, cum ar fi descărcarea de pornografie și trebuie să plătească imediat o amendă online prin introducerea unui număr de card de credit. Calculatorul rămâne „ținut ostatic” și blocat (cu excepția tastelor numerice de pe tastatură) până la răscumpărare.

Fig. 3.3. Ecran blocat de Ransomware

O altă variantă de ransomware afișează un avertisment fictiv că există o problemă a calculatorului, cum ar fi o infecție cu malware sau o defecțiune a hard diskului. Această variantă de ransomware comunică utilizatorilor că trebuie să cumpere imediat software suplimentar online pentru a rezolva problema, care de fapt nu există. Avertismentul pare să fie legitim, deoarece imită aspectul unui software autentic și în mod ilegal folosește mărci comerciale veridice sau pictograme. Exemplul de ransomware din figura 3.4 folosește scheme de culori și pictograme similare cu cele utilizate de software-ul Windows. Utilizatorii oferă numărul cardului de credit pentru a face achiziția, ca mai apoi să constate că sursele financiare au dispărut din cont.

Fig. 3.4. Ransomware care imită avertismentele Windows

Prin capacitatea sa de încărcare programele de malware șterg datele de pe calculator. Aceste acțiuni pot implica ștergerea fișierelor importante de date ale utilizatorului, cum ar fi documente sau fotografii, sau ștergerea elementelor vitale din fișierele sistemului de operare, astfel încât calculatorul să nu mai funcționeze corect [14].

Bomba logică

O bombă logică (figura 3.5) este un cod de calculator, care este de obicei adăugat la un program legitim, dar rămâne inactiv până când nu este declanșată de un anumit eveniment logic. Odată declanșat, programul șterge apoi datele sau efectuează alte activități rău intenționate. Un exemplu relevant este cazul unui angajat al guvernului SUA din Maryland, care a încercat să distrugă datele de pe 4000 de servere prin plasarea unui script de tip bombă logică care a fost programat să se activeze la 90 de zile după ce angajatul fusese concediat.

Fig. 3.5. Bomba logică (imagine reprezentativă)

Bombele logice sunt greu de detectat înainte de a fi declanșate. Acest lucru se datorează faptului că bombele logice sunt adesea integrate în programele de calculator mari, unele conținând zeci de mii de linii de cod, iar un angajat de încredere poate introduce cu ușurință câteva rânduri de cod de calculator într-un program voluminos fără ca nimeni să-l detecteze.

Sarcina utilă a unor tipuri de programe malware încearcă să modifice setările de securitate ale sistemului, astfel încât să poată fi făcute atacuri mai insidioase. Un tip de malware din această categorie se numește backdoor (figura 3.6). *Un backdoor oferă acces la un calculator, program sau serviciu care eludează orice protecție normală de securitate, iar când sunt instalate pe un calculator permit atacatorului să revină mai târziu și să ocolească setările de securitate*.

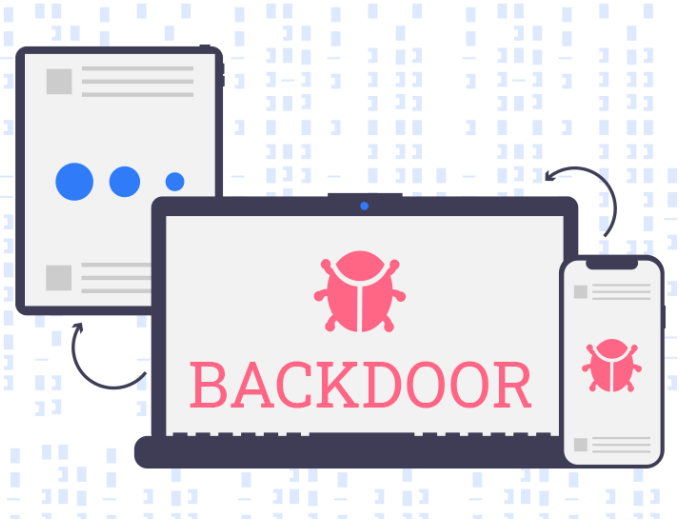

Fig. 3.6. Backdoor (imagine reprezentativă)

Programele malițioase permit controlul de la distanță a calculatoarelor infectate. Un calculator *robot (bot)* infectat este cunoscut sub numele de *zombie*. Când sute, mii sau chiar sute de mii de calculatoare *zombie* sunt adunate într-o rețea logică de calculatoare se creează o ***rețea bot*** (figura 3.7), cu care sub controlul atacatorilor se pot iniția diverse atacuri cibernetice.

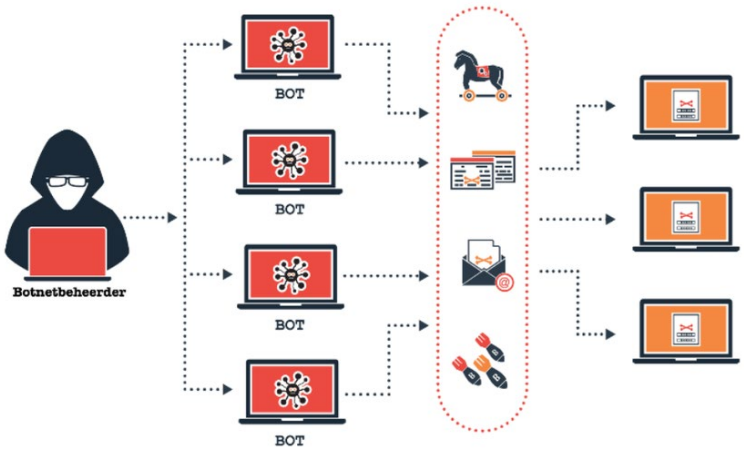

Fig. 3.7. Rețea de botnet

Calculatoarele zombi infectate așteaptă instrucțiuni prin comandă și control (C&C sau C2) de la atacatori cu privire la calculatoarele pe care să le atace. Mecanismul C&C obișnuit al rețelei botnet folosit astăzi este protocolul de transport hipertext (HTTP), care este protocolul standard pentru utilizarea Internetului [4]. De exemplu, un zombi poate primi instrucțiunile prin conectarea automată la un site web pe care îl operează botul sau către un site web terță-parte pe care au fost plasate informațiile despre atac. Zombi știe să interpreteze aceste informații drept comenzi (această din urmă tehnică are un avantaj în acest sens, atacatorul nu trebuie să aibă o afiliere cu site-ul respectiv). Prin utilizarea HTTP, traficul botnet poate fi mai dificil de detectat și blocat. Unele rețele bot chiar folosesc bloguri sau trimit comenzi de atac special codificate prin postări pe rețelele de socializare Twitter sau Facebook.

Tehnicile de răspândire des utilizate sunt prin conturi de e-mail Google false, care sunt configurate corespunzător, iar malware-ul zombi deține numele de utilizator și parola contului. Se creează apoi un mesaj de e-mail nefinalizat în Gmail, dar care nu va fi transmis niciodată. La orele stabilite, zombi se conectează la Gmail și citește conținutul mesajului nefinalizat pentru a primi instrucțiunile acestuia. Beneficiile acestei metode sunt că mesajul de e-mail nu este niciodată trimis, deci, nu există nicio înregistrare a acestuia și toate conținuturile Gmail sunt protejate astfel, încât să nu poată fi vizualizate de către străini. În tabelul 3.3 sunt enumerate câteva atacuri ce pot fi inițiate utilizând calculatoarele zombi.

Tabelul 3.3. Atacuri inițiate de rețelele de botnet

Nr.d/o	***Tipuri de atac***	***Descriere***
1	Spam	Rețelele bot sunt recunoscute pe scară largă ca sursă principală de e-mail spam. O rețea bot formată din mii de zombi permite unui atacator să trimită cantități masive de spam.
2	Răspândire malware	Rețelele bot pot fi folosite pentru a răspândi programe malware și pentru a crea noi zombi și rețele bot. Zombii au capacitatea de a se descărca și executa un fișier trimis de atacator.
3	Manipulare sondaje online	Deoarece fiecare zombi are o adresă IP, fiecare „vot” făcut de către un zombie va avea aceeași credibilitate ca și un vot exprimat de o persoană reală. Jocurile online pot fi manipulate în mod similar.
4	Întreruperea serviciilor (DoS/DDoS)	Rețelele bot pot inunda un server web cu mii de solicitări și îl pot copleși astfel, încât serverul nu va mai putea răspunde cererilor legitime.

3.3. Analiză și protecție antimalware

Analiza malware este arta de a diseca programele malițioase pentru a înțelege cum funcționează, cum pot fi identificate și cum pot fi învinse sau eliminate.

Cu milioane de programe rău intenționate întâlnite în fiecare zi, analiza programelor malware este esențială pentru oricine răspunde la incidente de securitate informatică. Pentru analiza malware se utilizează un set de bază de instrumente și tehnici.

Există două abordări fundamentale ale analizei malware: ***statică*** și ***dinamică*** [11]. Analiza statică implică examinarea malware-ului fără a-l rula. Analiza dinamică implică rularea malware-ului.

Analiza statică de bază constă în examinarea fișierului executabil fără a vizualiza instrucțiuni reale din fișier. Analiza statică de bază poate confirma dacă un fișier este rău intenționat, furnizează informații despre funcționalitatea acestuia și, uneori, oferă informații care permit producerea semnăturilor simple de rețea. Analiza statică de bază este simplă și poate fi rapidă, dar este în mare parte ineficientă împotriva malware-ului sofisticat și poate pierde comportamente importante.

Tehnicile de bază de analiză dinamică implică rularea malware-ului și observarea comportamentului acestuia asupra sistemului pentru a elimina infecția, a produce eficient semnături. Cu toate acestea, înainte de a putea rula malware în siguranță, trebuie să fie configurat un mediu care va permite studierea malware-ului ce rulează fără riscuri de deteriorare a sistemului sau a rețelei. Ca și tehnicile de analiză statică de bază, tehnicile de analiză dinamică pot fi folosite de majoritatea oamenilor fără cunoștințe de programare aprofundate.

Principalele metode de protecție împotriva programelor malware sunt:

- *Programele antivirus* - majoritatea programelor antivirus captează cele mai răspândite forme de malware. Cu toate acestea, infractorii cibernetici dezvoltă și implementează malware noi în fiecare zi. Prin urmare, cheia unei soluții antivirus eficiente este actualizarea permanentă a semnăturilor malware, care se conțin în baza de date a antivirusului. O semnătură este ca o amprentă, identificând caracteristicile unui malware și generează alerte sau blochează malware-ul în cazul când detectează o semnătură similară.
- *Actualizare software* – multe forme de malware își ating obiectivele prin exploatarea vulnerabilităților din software atât în sistemul de operare, cât și în aplicații. Deși vulnerabilitățile sistemului de operare au fost principala sursă de probleme timp îndelungat, vulnerabilitățile la nivel de aplicație de astăzi au cel mai mare risc, deoarece nu sunt actualizate în timp real.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Ce malware necesită a fi transportat de utilizator de pe un dispozitiv pe altul?
2. Care sunt acțiunile realizate de către virusul informatic?
3. Descrieți tipurile de viruși în dependență de cod și programele afectate?
4. Cum pot fi clasificate tipurile de malware? Cum diferă viermii de viruși? *Calul troian* este purtător de viruși sau de viermi?
5. De ce polimorfismul provoacă o îngrijorare mai mare decât malware-ul tradițional?
6. Cum afectează polimorfismul detectarea malware-ului?
7. După ce criterii sunt clasificate programele spyware?
8. Descrieți succint atacurile care pot fi inițiate de rețelele de botnet? Ce efecte pot produce?
9. Enumerați extensiile fișierelor care pot fi afectate în SO Windows.
10. Realizați un studiu al resurselor Internet pentru o analiză comparativă a celor mai frecvent întâlnite malware în ultimii 3 ani și a daunelor cauzate de astfel de software.