Lecția 3: Software malițios (Malware)

Tema: Malware și inginerie socială
Universitatea Tehnică a Moldovei
Lector: Maxim Masiutin, Asistent universitar

Introducere

Bună ziua tuturor. Astăzi intrăm în lumea software-ului malițios, cunoscut sub denumirea de malware. Aceasta este una dintre cele mai dinamice domenii ale securității cibernetice, cu noi amenințări care apar zilnic și atacatori care își evoluează constant tehnicile.

Permiteți-mi să încep cu câteva cifre care ilustrează amploarea problemei. Conform SonicWall, o companie de securitate a rețelelor, în 2025 au fost înregistrate la nivel global peste 783 de milioane de tentative de atac ransomware, față de 658 de milioane în 2024. Proiecțiile pentru 2026 sugerează că acest număr ar putea depăși un miliard de tentative. Iar ransomware-ul este doar un tip de malware.

Cyble, o companie de informații privind amenințările cibernetice, a observat 57 de grupuri noi de ransomware și 27 de grupuri noi de extorcare în 2025, împreună cu peste 350 de tulpini noi de ransomware. Ecosistemul malware este vast, sofisticat și foarte profitabil pentru infractori. Înțelegerea modului în care funcționează malware-ul este esențială pentru apărarea împotriva acestuia.

Partea 1: Taxonomia malware-ului

Malware-ul este orice software conceput intenționat pentru a provoca daune unui calculator, server, rețele sau utilizator. Termenul combină cuvintele „malicious" (malițios) și „software". Să examinăm categoriile principale.

Viruși

Un **virus** este un program malițios care se atașează la un program sau fișier legitim și se răspândește atunci când acel program este executat. La fel ca virușii biologici, virușii informatici nu se pot propaga fără o gazdă.

Caracteristici:

- Necesită acțiune din partea utilizatorului pentru a se răspândi (rularea programului infectat)
- Se atașează la fișiere legitime
- Poate deteriora sau modifica fișiere
- Se poate răspândi prin medii infectate, atașamente de e-mail, descărcări

Tipuri de viruși:

- **Infectori de fișiere**: Se atașează la fișiere executabile
- **Viruși de sector de boot**: Infectează înregistrarea de boot principală
- **Viruși macro**: Se ascund în macrocomenzile documentelor (Word, Excel)
- **Viruși polimorfi**: Își schimbă codul pentru a evita detectarea
- **Viruși metamorfici**: Se rescriu complet

Notă istorică: Virușii au fost dominanți în anii 1990 și începutul anilor 2000, dar au devenit mai puțin comuni pe măsură ce alte tipuri de malware s-au dovedit mai eficiente pentru atacatori.

Viermi

Un **vierme** este un software malițios care se auto-replică și se răspândește automat prin rețele, fără a necesita acțiunea utilizatorului sau un program gazdă. Acest lucru face viermii deosebit de periculoși, deoarece se pot răspândi rapid.

Caracteristici:

- Se auto-replică
- Se răspândește automat prin rețea
- Nu necesită un program gazdă
- Poate consuma lățime de bandă și resurse de sistem
- Exploatează adesea vulnerabilități pentru propagare

Exemple celebre:

- **Morris Worm (1988)**: Unul dintre primii viermi, a blocat 10% din calculatoarele conectate la internet
- **Code Red (2001)**: A exploatat o vulnerabilitate IIS, infectând 359.000 de calculatoare în 14 ore
- **SQL Slammer (2003)**: A infectat 75.000 de servere în 10 minute
- **Conficker (2008)**: A infectat milioane de calculatoare, fiind activ și în prezent
- **WannaCry (2017)**: A combinat răspândirea de tip vierme cu o sarcină utilă de tip ransomware

Troieni

Un **troian** (sau Cal Troian) este un software malițios deghizat în software legitim. Utilizatorii sunt păcăliți să îl instaleze, crezând că primesc ceva util.

Denumit după mitul grecesc în care soldații s-au ascuns într-un cal de lemn pentru a intra în Troia, troienii par inofensivi, dar conțin funcționalitate malițioasă ascunsă.

Caracteristici:

- Deghizat în software legitim
- Necesită instalare de către utilizator
- Nu se auto-replică
- Oferă adesea acces de tip backdoor
- Poate avea funcționalitate aparent legitimă

Tipuri de troieni:

- **Troieni de acces la distanță (RAT)**: Oferă control de la distanță atacatorilor
- **Troieni bancari**: Fură credențiale financiare
- **Troieni de descărcare**: Descarcă malware suplimentar
- **Troieni spion**: Monitorizează activitatea utilizatorului
- **Troieni de furt de jocuri**: Fură credențialele conturilor de jocuri

Ransomware

Ransomware-ul criptează fișierele victimei sau blochează sistemele, cerând plata (de obicei în criptomonedă) pentru restaurare. Acesta a devenit amenințarea malware dominantă în ultimii ani.

Caracteristici:

- Criptează fișierele sau blochează sistemele
- Cere plata unei răscumpărări
- Utilizează adesea criptare puternică
- Poate avea cereri cu limită de timp
- Vizează din ce în ce mai mult organizațiile în locul persoanelor fizice

Evoluția ransomware-ului:

- **Ransomware timpuriu**: Blocaje simple de ecran
- **CryptoLocker (2013)**: Primul ransomware de criptare larg răspândit cu succes
- **Extorcare dublă (2019+)**: Furtul datelor înainte de criptare, amenințarea cu publicarea
- **Extorcare triplă**: Adăugarea atacurilor DDoS sau contactarea clienților victimelor

- **Ransomware ca Serviciu (RaaS)**: Model de afaceri criminal

Statisticile sunt alarmante: conform Cyble, atacurile ransomware raportate public au crescut la 7.200 în 2025, comparativ cu 4.900 în 2024, o creștere de 47 de procente. Conform Coveware, o companie de răspuns la incidente ransomware, peste 60 de procente din atacurile ransomware includ acum componente de exfiltrare a datelor.

Conform Raportului IBM/Ponemon Cost of a Data Breach din 2025, costul total mediu al unui atac ransomware, incluzând timpul de nefuncționare, recuperarea și prejudiciul reputațional, variază între 1,8 milioane și 5 milioane de dolari per incident. Sectoarele sănătății și producției se confruntă cu cele mai mari costuri din cauza perturbării operaționale.

Spyware

Spyware-ul monitorizează în secret activitatea utilizatorului și colectează informații fără consimțământ. Poate urmări obiceiurile de navigare, captura tastele apăsate sau colecta informații personale.

Caracteristici:

- Operează pe ascuns
- Colectează informații despre utilizator
- Poate încetini performanța sistemului
- Adesea inclus în pachete cu software gratuit
- Dificil de detectat

Tipuri:

- **Keylogger-e**: Înregistrează tastele apăsate pentru a captura parole
- **Captură de ecran**: Realizează capturi de ecran ale activității utilizatorului
- **Hijacker-e de browser**: Modifică setările browserului, redirecționează căutările
- **Cookie-uri de urmărire**: Monitorizează comportamentul de navigare
- **Spyware comercial**: Instrumente precum Pegasus utilizate pentru supraveghere

Rootkit-uri

Un **rootkit** este un software malițios conceput pentru a oferi acces privilegiat, ascunzând în același timp prezența sa față de instrumentele de detectare. Numele provine de la sistemele Unix, unde „root" este contul de administrator.

Caracteristici:

- Se ascunde de sistemul de operare
- Oferă acces persistent
- Extrem de dificil de detectat

- Poate modifica componentele sistemului de operare
- Adesea necesită reinstalarea completă a sistemului pentru eliminare

Tipuri:

- **Rootkit-uri de mod utilizator**: Operează la nivel de aplicație
- **Rootkit-uri de mod kernel**: Operează la nivelul nucleului sistemului de operare
- **Bootkit-uri**: Infectează procesul de boot, se încarcă înainte de sistemul de operare
- **Rootkit-uri de firmware**: Se ascund în firmware-ul hardware

Detectarea rootkit-urilor necesită adesea pornirea de pe un mediu curat și scanarea sistemului din exterior.

Bootkit-uri

Un **bootkit** este un rootkit avansat care infectează procesul de boot, încărcându-se înainte de sistemul de operare. Acest lucru îi permite să evite detectarea de către software-ul de securitate care se încarcă după sistemul de operare.

Bootkit-urile vizează:

- Master Boot Record (MBR)
- Volume Boot Record (VBR)
- Firmware UEFI

Deoarece bootkit-urile se încarcă înainte de sistemul de operare, pot intercepta și modifica orice funcție a sistemului de operare, ceea ce le face extrem de periculoase.

Adware

Adware-ul afișează reclame nedorite pe sistemele utilizatorilor. Deși uneori este considerat mai puțin periculos decât alte tipuri de malware, adware-ul poate degrada performanța sistemului, urmări comportamentul utilizatorului și servi ca vector pentru malware mai periculos.

Caracteristici:

- Afișează reclame nedorite
- Poate urmări comportamentul de navigare
- Adesea inclus în pachete cu software gratuit
- Poate redirecționa rezultatele căutărilor
- Poate instala software nedorit suplimentar

Malware de criptominare neautorizată (Cryptojacking)

Malware-ul de tip **cryptojacking** utilizează sistemele victimelor pentru a mina criptomonedă fără consimțământ. Deși nu este distructiv, consumă resurse de calcul și electricitate.

Caracteristici:

- Minează criptomonedă
- Consumă resurse CPU/GPU
- Crește costurile cu electricitatea
- Poate cauza deteriorarea hardware-ului din cauza suprasolicitării
- Adesea livrat prin exploit-uri bazate pe browser

Partea 2: Vectori de infectare și propagare

Înțelegerea modului în care malware-ul ajunge la sisteme ne ajută să implementăm apărări eficiente.

Livrare prin e-mail

E-mailul rămâne cel mai comun mecanism de livrare a malware-ului:

- **Atașamente malițioase**: Documente cu macrocomenzi, fișiere executabile
- **Linkuri malițioase**: Care conduc la kituri de exploit sau descărcări de malware
- **Fișiere arhivă**: Fișiere ZIP, RAR care conțin malware
- **HTML smuggling**: Codificarea malware-ului în atașamente HTML

Descărcări automate (Drive-By Downloads)

Utilizatorii se infectează pur și simplu vizitând site-uri web compromise:

- Kiturile de exploit vizează vulnerabilitățile browserului
- Nu este necesară nicio interacțiune din partea utilizatorului în afara vizitării paginii
- Pot utiliza site-uri legitime care au fost compromise
- Malvertising-ul livrează malware prin rețele de publicitate

Vulnerabilități software

Malware-ul exploatează vulnerabilități în software:

- Sisteme de operare neactualizate

- Aplicații învechite
- Vulnerabilități ale plugin-urilor de browser
- Exploit-uri de tip zero-day

Medii amovibile

Unitățile USB și alte medii amovibile pot răspândi malware:

- Funcționalitatea autorun (în mare parte dezactivată în prezent)
- Inginerie socială pentru a rula fișiere malițioase
- Infecții la nivel de firmware

Propagare prin rețea

Viermii și alt malware se răspândesc prin rețele:

- Exploatarea serviciilor vulnerabile
- Utilizarea credențialelor furate
- Valorificarea relațiilor de încredere

Lanțul de aprovizionare

Malware-ul poate fi introdus prin lanțul de aprovizionare software:

- Actualizări software compromise
- Componente open-source infectate
- Instrumente de dezvoltare troianizate

Conform Raportului Verizon Data Breach Investigations Report (DBIR) din 2025, 29 de procente din infecțiile ransomware au provenit prin furnizori terți, față de 17 procente în 2024.

Partea 3: Analiză aprofundată a ransomware-ului

Având în vedere prevalența și impactul ransomware-ului, să îl examinăm mai în detaliu.

Ransomware ca Serviciu (RaaS)

Modelul RaaS a transformat ransomware-ul într-o industrie criminală:

Cum funcționează RaaS:

1. Dezvoltatorii creează ransomware-ul și infrastructura
2. Afiliații plătesc sau închiriază accesul la platformă
3. Afiliații efectuează atacuri folosind instrumentele
4. Profiturile sunt împărțite (de obicei 70-80% pentru afiliat)

Beneficii pentru infractori:

- Dezvoltatorii profită fără a efectua atacuri
- Afiliații au nevoie de competențe tehnice minime
- Operațiuni criminale scalabile
- Infrastructură și suport partajate

Acest model a „democratizat criminalitatea cibernetică într-un grad fără precedent." Oricine cu cunoștințe de bază de internet poate utiliza aceste servicii.

Extorcare dublă și triplă

Ransomware-ul modern depășește simpla criptare:

Extorcare dublă:

1. Atacatorii fură datele sensibile
2. Atacatorii criptează fișierele
3. Cer plata pentru decriptare ȘI prevenirea publicării datelor
4. Chiar dacă există copii de siguranță, amenințarea expunerii datelor rămâne

Extorcare triplă:

1. Toate cele de mai sus
2. Plus atacuri DDoS împotriva victimelor
3. Plus contactarea clienților sau partenerilor victimelor
4. Tactici suplimentare de presiune

Conform Raportului Sophos State of Ransomware din 2025, peste 60 de procente din atacurile ransomware includ acum exfiltrarea datelor. Majoritatea grupurilor noi de ransomware adoptă imediat extorcarea dublă, deoarece aceasta crește randamentul investiției și reduce puterea de negociere a victimei.

Ciclul de viață al unui atac ransomware

Progresia tipică a unui atac ransomware:

1. **Accesul inițial**: Phishing, servicii vulnerabile, RDP
2. **Persistența**: Instalarea de backdoor-uri, crearea de conturi
3. **Escaladarea privilegiilor**: Obținerea accesului de administrator

4. **Evitarea apărării**: Dezactivarea instrumentelor de securitate
5. **Colectarea credențialelor**: Furtul parolelor
6. **Mișcarea laterală**: Răspândirea în rețea
7. **Colectarea datelor**: Identificarea și furtul datelor valoroase
8. **Exfiltrarea datelor**: Extragerea datelor către infrastructura atacatorului
9. **Impactul**: Implementarea ransomware-ului, criptarea fișierelor
10. **Extorcarea**: Cererea de plată, amenințarea cu publicarea datelor

Operatorii moderni de ransomware petrec adesea zile sau săptămâni în interiorul rețelelor înainte de implementarea criptării.

Tactici emergente de ransomware pentru 2026

Tendințe noi apar:

- **Oferte DDoS-as-a-Service**: Presiune suplimentară asupra victimelor
- **Recrutarea insiderilor**: Plata angajaților pentru a furniza acces
- **Exploatarea lucrătorilor temporari**: Recrutarea de complici online
- **Atacuri asistate de IA**: Selecție automată a victimelor și personalizare
- **Extorcare prin scurgerea datelor fără criptare**: Unele grupuri renunță complet la criptare

---

Partea 4: Software malițios fără fișiere și tehnici de tip Living-Off-the-Land

Malware-ul tradițional scrie fișiere pe disc, dar atacatorii moderni utilizează din ce în ce mai mult tehnici fără fișiere.

Ce este software-ul malițios fără fișiere?

Software-ul malițios fără fișiere operează în întregime în memorie, fără a scrie fișiere persistente pe disc. Acest lucru îl face extrem de dificil de detectat cu antivirusul tradițional.

Caracteristici:

- Niciun fișier scris pe disc
- Rezidă în memorie
- Utilizează instrumente de sistem legitime
- Supraviețuiește doar până la repornire (dacă nu se obține persistența)

- Evită detectarea bazată pe semnături

Conform Raportului ENISA Threat Landscape din 2025, atacurile malware fără fișiere au crescut cu 33 de procente din 2023 până în 2025, vizând punctele oarbe ale detectării la nivelul punctelor terminale.

Tehnici de tip Living-Off-the-Land (LOtL)

Atacatorii utilizează instrumente de sistem legitime în scopuri malițioase:

Instrumente frecvent exploatate:

- **PowerShell**: Scripting și automatizare
- **WMI (Windows Management Instrumentation)**: Administrarea sistemului
- **certutil**: Utilitar de certificate folosit abuziv pentru descărcări
- **bitsadmin**: Serviciu de transfer în fundal
- **mshta**: Execută fișiere HTA
- **regsvr32**: Înregistrează componente COM

De ce LOtL este eficient:

- Instrumentele sunt deja prezente pe sisteme
- Acțiunile pot părea legitime
- Dificil de distins utilizarea malițioasă
- Nu se pot bloca pur și simplu aceste instrumente
- Antivirusul tradițional se concentrează pe fișiere malițioase

Provocări de detectare

Atacurile fără fișiere și LOtL necesită abordări diferite de detectare:

- Analiza comportamentală în loc de semnături
- Monitorizarea liniei de comandă
- Logarea blocurilor de script
- Analiza memoriei
- Analitica comportamentului utilizatorilor și entităților (UEBA)

Partea 5: Bazele analizei malware

Profesioniștii în securitate analizează malware-ul pentru a înțelege amenințările și a dezvolta apărări.

Analiza statică

Analiza statică examinează malware-ul fără a-l executa:

Tehnici:

- **Examinarea metadatelor fișierului**: Anteturi, marcaje temporale, informații despre compilator
- **Extragerea șirurilor de caractere**: Căutarea de URL-uri, adrese IP, comenzi
- **Analiza codului**: Dezasamblare și decompilare
- **Calculul hash-urilor**: Generarea indicatorilor de compromitere (IOC) pentru detectare
- **Detectarea packerelor**: Identificarea metodelor de obfuscare

Instrumente:

- PEStudio (executabile Windows)
- Comanda strings
- IDA Pro, Ghidra (dezasambloare)
- VirusTotal (analiză multi-scanner)

Avantaje:

- Sigură (malware-ul nu este executat)
- Poate dezvălui capabilitățile fără a le declanșa

Limitări:

- Obfuscarea și împachetarea complică analiza
- Nu se poate observa comportamentul în timpul execuției

Analiza dinamică

Analiza dinamică execută malware-ul într-un mediu controlat:

Tehnici:

- **Execuție în sandbox**: Rulare în mediu virtual izolat
- **Monitorizarea proceselor**: Observarea creării și activității proceselor
- **Monitorizarea sistemului de fișiere**: Urmărirea operațiunilor cu fișiere
- **Monitorizarea registrului**: Supravegherea modificărilor de configurare
- **Monitorizarea rețelei**: Capturarea comunicațiilor
- **Monitorizarea API**: Logarea apelurilor de sistem

Instrumente:

- Cuckoo Sandbox
- Any.Run (sandbox online)

- Process Monitor
- Wireshark
- API Monitor

Avantaje:

- Dezvăluie comportamentul real
- Poate observa codul despachetizat

Limitări:

- Malware-ul poate detecta sandbox-ul și își poate modifica comportamentul
- Unele comportamente se declanșează doar în condiții specifice
- Riscuri dacă izolarea eșuează

Evitarea sandbox-ului

Malware-ul sofisticat detectează mediile de analiză:

Tehnici de detectare:

- Verificarea artefactelor VM (drivere, chei de registru)
- Atacuri de temporizare (pauze pentru a depăși durata analizei)
- Cerințe de interacțiune cu utilizatorul
- Verificări de mediu (nume utilizator, nume mașină)
- Amprentare hardware

Contramăsuri:

- Medii de analiză pe hardware fizic (bare-metal)
- Configurații de sistem realiste
- Timpi de analiză extinși
- Simularea interacțiunii umane

Partea 6: Tehnologii defensive

Acum să examinăm tehnologiile care apără împotriva malware-ului.

Detectarea bazată pe semnături

Antivirusul tradițional se bazează pe semnături:

- Bază de date cu modele cunoscute de malware

- Fișierele sunt comparate cu semnăturile
- Rapidă și precisă pentru amenințări cunoscute
- Necesită actualizări regulate

Limitări:

- Nu poate detecta malware nou (de tip zero-day)
- Ușor de evitat prin modificare
- Ineficientă împotriva atacurilor fără fișiere

Detectarea euristică

Euristicile identifică malware-ul prin modele de comportament:

- Reguli bazate pe caracteristici suspecte
- Poate detecta variante ale malware-ului cunoscut
- Poate identifica unele amenințări noi
- Rată mai mare de fals pozitiv decât semnăturile

Detectarea comportamentală

Soluțiile moderne monitorizează comportamentul:

- Supravegherea acțiunilor suspecte în timp real
- Detectarea malware-ului prin ceea ce face, nu prin cum arată
- Eficientă împotriva atacurilor fără fișiere și LOtL
- Poate interveni înainte de producerea daunelor

Indicatori comportamentali:

- Modificarea masivă a fișierelor
- Activități de criptare
- Injectarea în procese
- Modificări ale registrului
- Anomalii de rețea

Detectarea prin învățare automată

IA/ML îmbunătățește detectarea malware-ului:

- Antrenarea modelelor pe caracteristicile malware-ului
- Identificarea tiparelor pe care oamenii le-ar putea rata
- Adaptare la amenințări noi

- Reducerea dependenței de semnături

Limitări:

- Necesită date de antrenament de calitate
- Atacurile adversariale pot evita ML
- Poate produce fals pozitive
- Provocări de explicabilitate

Detecție și răspuns la punctele terminale (EDR)

EDR oferă protecție cuprinzătoare a punctelor terminale:

- Monitorizare continuă
- Analiză comportamentală
- Capabilități de vânătoare de amenințări (threat hunting)
- Instrumente de răspuns la incidente
- Colectare de date forensice

EDR depășește prevenția pentru a detecta și răspunde amenințărilor care evită apărările inițiale.

Sandboxing

Sandboxing-ul izolează conținutul potențial periculos:

- Atașamentele de e-mail sunt detonated în siguranță
- Descărcările sunt analizate înainte de livrare
- Fișierele suspecte sunt executate în izolare
- Comportamentul este observat fără risc

Partea 7: Strategii practice de apărare împotriva malware-ului

---

Permiteți-mi să vă prezint strategii practice de apărare împotriva malware-ului.

Apărare în profunzime

Stratificarea mai multor protecții:

1. Gateway de securitate e-mail

2. Filtrare web
3. Protecție la punctul terminal
4. Monitorizarea rețelei
5. Instruirea utilizatorilor
6. Backup și recuperare

Gestionarea actualizărilor

Mențineți sistemele actualizate:

- Prioritizați vulnerabilitățile critice
- Testați actualizările înainte de implementare
- Utilizați actualizări automate acolo unde este posibil
- Urmăriți starea actualizărilor

Principiul privilegiului minim

Limitați permisiunile utilizatorilor și proceselor:

- Utilizatorii nu ar trebui să aibă drepturi de administrator pentru munca zilnică
- Aplicațiile rulează cu permisiuni minime
- Reduce impactul malware-ului în caz de succes

Lista albă a aplicațiilor

Permiteți doar aplicațiile aprobate:

- Blocați execuția programelor necunoscute
- Foarte eficientă, dar necesită efort de administrare
- De luat în considerare pentru mediile cu securitate ridicată

Strategia de backup

Pregătiți-vă pentru ransomware:

- Backup-uri regulate, automatizate
- Copii de backup offline sau izolate fizic (air-gapped)
- Testați procedurile de restaurare
- Backup-uri imuabile acolo unde este posibil
- Regula 3-2-1: 3 copii, 2 tipuri de medii, 1 în afara locației

Segmentarea rețelei

Limitați răspândirea malware-ului:

- Separați sistemele critice
- Controlați traficul între segmente
- Monitorizați tentativele de mișcare laterală

Instruirea utilizatorilor

Oamenii sunt adesea veriga cea mai slabă:

- Conștientizarea phishing-ului
- Practici de navigare sigură
- Raportarea activității suspecte
- Instruire periodică de reamintire

Concluzie

Astăzi am acoperit lumea software-ului malițios:

1. **Taxonomia malware-ului**: Viruși, viermi, troieni, ransomware, spyware, rootkit-uri și altele
2. **Vectori de infectare**: E-mail, descărcări automate, vulnerabilități, medii amovibile, lanțul de aprovizionare
3. **Evoluția ransomware-ului**: Modelul RaaS, extorcare dublă/triplă, tactici emergente
4. **Software malițios fără fișiere**: Amenințări rezidente în memorie și tehnici de tip Living-off-the-Land
5. **Metode de analiză**: Abordări de analiză statică și dinamică
6. **Tehnologii defensive**: Semnături, euristici, comportament, ML, EDR, sandboxing
7. **Strategii de apărare**: Abordare stratificată, actualizări, privilegiu minim, backup-uri

În lecția următoare, vom examina ingineria socială, unde atacatorii vizează elementul uman în locul vulnerabilităților tehnice.

Întrebări de discuție

1. Ar trebui organizațiile să plătească cererile de ransomware? Ce factori ar trebui să influențeze această decizie?
2. Cum putem echilibra securitatea cu uzabilitatea atunci când blocăm conținut potențial malițios?
3. Ce rol ar trebui să joace guvernele în combaterea ransomware-ului?

Vă mulțumesc pentru atenție. Ne vedem data viitoare.

Întrebări de recapitulare

1. Distingeți între viruși, viermi și troieni. Cum diferă metodele lor de propagare?
2. Explicați modelul Ransomware ca Serviciu (RaaS) și de ce a făcut ransomware-ul mai prevalent.
3. Ce este extorcarea dublă în ransomware și cum schimbă calculul riscului pentru organizații?
4. Descrieți software-ul malițios fără fișiere și tehnicile de tip Living-off-the-Land. De ce sunt dificil de detectat?
5. Comparați analiza statică și cea dinamică a malware-ului. Care sunt punctele forte și limitările fiecărei abordări?
6. Cum diferă soluțiile moderne EDR de antivirusul tradițional bazat pe semnături?
7. Ce este evitarea sandbox-ului și ce tehnici folosesc autorii de malware pentru a evita analiza?
8. Schițați o strategie de apărare în profunzime specifică pentru protecția împotriva malware-ului.

Termeni cheie

- **Adware**: Software care afișează reclame nedorite
- **Bootkit**: Software malițios care infectează procesul de boot pentru a se încărca înainte de sistemul de operare
- **Cryptojacking**: Utilizarea neautorizată a resurselor de calcul pentru a mina criptomonedă
- **Extorcare dublă**: O tactică ransomware care combină criptarea datelor cu furtul de date, amenințând cu publicarea datelor furate dacă răscumpărarea nu este plătită

- **Descărcare automată (Drive-By Download)**: Software malițios descărcat automat la vizitarea unui site web compromis
- **Analiză dinamică**: Procesul de analizare a comportamentului malware-ului prin executarea acestuia într-un mediu controlat
- **EDR**: Detecție și Răspuns la Punctele Terminale, securitate avansată a punctelor terminale care oferă vizibilitate și capacitate de răspuns
- **Software malițios fără fișiere**: Software malițios care operează în întregime în memorie, fără a scrie fișiere pe disc
- **Living off the Land (LOtL)**: Utilizarea instrumentelor de sistem legitime în scopuri malițioase
- **Ransomware**: Software malițios care criptează datele și cere plata pentru decriptare
- **Ransomware ca Serviciu (RaaS)**: Un model de afaceri criminal care furnizează instrumente ransomware afiliaților
- **Rootkit**: Software malițios conceput pentru a-și ascunde prezența și a oferi acces privilegiat continuu
- **Sandbox**: Un mediu izolat pentru analiza în siguranță a codului suspect
- **Evitarea sandbox-ului**: Tehnici utilizate de malware pentru a detecta și evita analiza în medii sandbox
- **Spyware**: Software care colectează în mod ascuns informații despre un utilizator
- **Analiză statică**: Procesul de analiză a malware-ului fără a-l executa, examinând structura codului și semnăturile
- **Troian**: Software malițios deghizat în software legitim
- **Virus**: Software malițios care se atașează la programe și se replică atunci când programul gazdă este executat
- **Vierme**: Software malițios care se auto-replică și se răspândește prin rețele fără interacțiunea utilizatorului

Referințe și lectură suplimentară

- NIST SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- MITRE ATT&CK for Enterprise (attack.mitre.org)
- CISA Stop Ransomware Resources (stopransomware.gov)
- AV-TEST Institute Reports (av-test.org)
- VirusTotal Documentation (virustotal.com)