SECURITATEA PE INTERNET

ANDREI FLORIN CIOANCĂ

SECURITATEA INFORMATICĂ ESTE O RAMURĂ A INFORMATICII CARE SE OCUPĂ CU IDENTIFICAREA RISCURILOR IMPLICATE DE FOLOSIREA DISPOZITIVELOR INFORMATIVE, CUM SUNT CALCULATOARE, SMARTPHONE-URI, DAR ȘI REȚELE DE CALCULATOARE ATÂT PUBLICE CÂT ȘI PRIVATE, ȘI CU OFERIREA DE SOLUȚII PENTRU ÎNLĂTURAREA LOR.

VIRUS INFORMATIC

- Virusul informatic este în general un program care se instalează singur, fără voia utilizatorului, și poate provoca pagube atât în sistemul de operare cât și în elementele hardware (fizice) ale computerului. Viruși hardware: sunt cei care afectează discul dur, discul flexibil și memoria.
- Viruși software: afectează fișierele si programele aflate in memorie sau pe disc, inclusiv sistemul de operare sau componente ale acestuia.
- Câteva dintre efectele pe care le generează virușii software:
- distrugerea unor fișiere;
- modificarea dimensiunii fișierelor;

- ștergerea totală a informaților de pe disc, inclusiv formatarea acestuia;
- distrugerea tabelei de alocare a fișierelor, care duce la imposibilitatea citirii informației de pe disc;
- încetinirea vitezei de lucru (utilă) a calculatorului, până la blocarea acestuia;
- înmulțirea fișierelor până la umplerea memoriei;

ISTORIA VIRUȘILOR DIN INFORMATICĂ

- 1949 Sunt puse pentru prima oara bazele teoriilor legate de programele care se autoreproduc cu mult mai mult .
- 1983 In teza sa de doctorat, Fred Cohen definește pentru prima oara formal un virus de calculator ca fiind "un program ce poate afecta alte programe de calculator, modificandu-le intr-un mod care presupune abordarea unor copii evoluate ale lor."
- 1986 Doi programatori, Basit si Amjad, inlocuiesc codul executabil din sectorul boot al unui floppy-disk cu propriul lor cod, care infecta fiecare floppy de 360 Kb accesat pe orice drive. Floppy-urile infectate aveau "© Brain" ca eticheta de disc (volume label).
- 1987 Scapa din lesa unul dintre cei mai cunoscuti virusi: Jerusalem. Activat in fiecare vineri 13, virusul afecteaza fisierele .exe si .com si sterge toate programele rulate in cursul acelei zile.
- 1990 Symantec lanseaza pe piata Norton AntiVirus, unul dintre primele programe antivirus dezvoltate de catre una dintre marile companii.
- 1991 Tequila este primul virus polimorf cu raspandire pe scara larga gasit "in the wild". Virusii polimorfi fac ca detectarea lor de catre scanerele de virusi sa fie dificila, prin schimbarea modul de actiune cu fiecare noua infectie.

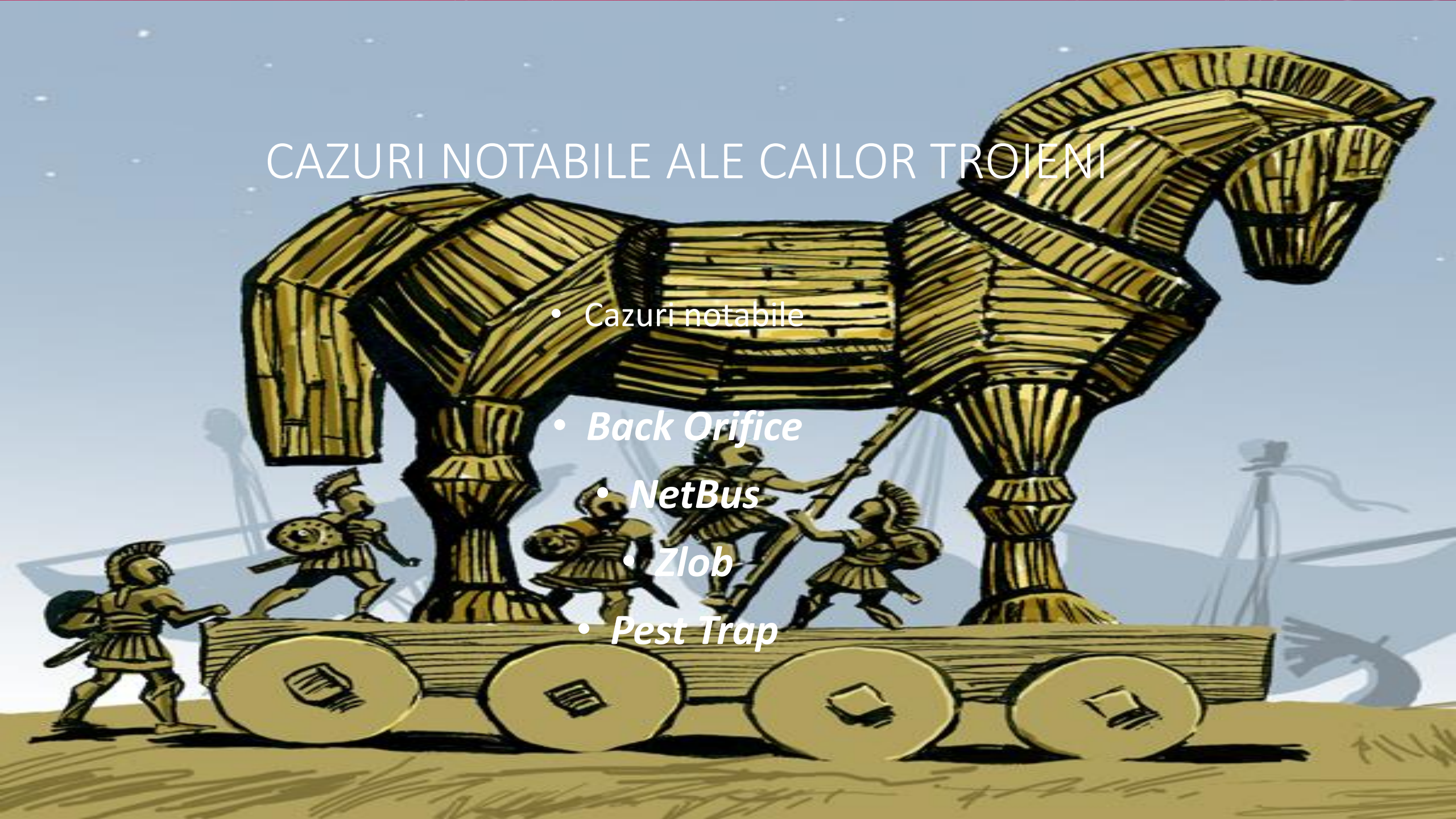
- 1992 Exista 1300 de virusi, cu aproape 420% mai multi decat in decembrie 1990. Previziunile sumbre ale virusului Michelangelo ameninta colapsul a circa 5 milioane de calculatoare pe data de 6 martie. Insa doar 5,000-10,000 de calculatoare se intampla sa "dea coltul".
- 1995 Word Concept, virus de Microsoft Word, devine unul dintre cei mai raspanditi virusi din anii '90..
- "Bubble Boy" este primul virus care nu mai depinde de deschiderea atașamentului pentru a se executa. De îndată ce utilizatorul deschide programul de e-mail, Bubble Boy se și activează.

- 2000 "Love Bug", cunoscut și sub numele de ILOVEYOU, se răspândește prin *Outlook*, asemănător modului de răspândire al Melissei. Acest virus e primit ca un atașament de tip .VBS, șterge fișiere, inclusiv de tip MP3, MP2 și JPG, și trimite *username*-uri și parole găsite în sistem autorului virusului. "W97M.Resume.A", o nouă variantă a Melissei, este "*in the wild*". Virusul se comportă cam ca Melissa, folosindu-se de un macro *Word* pentru a infecta *Outlook*-ul și pentru a se răspândi. Virusul "Stages", deghizat într-un e-mail-glumă despre etapele vieții, se răspândește prin Internet. rareori întâlnit la virușii anteriori, Stages este ascuns într-un atașament cu extensie falsă de tip .txt, momind utilizatorii să-l deschidă. Până la apariția sa, fișierele de tip text erau considerate fișiere sigure.

CAL TROIAN

- Un **cal troian** (în engleză: **trojan horse**, cunoscut de asemenea doar ca **troian**) în cazul software-ul computerelor (având numele derivat din legenda calului troian) descrie un anumit tip de program spion (care este la rândul său un tip de software rău intenționat), care apare că ar realiza ceva util, dar care în realitate realizează funcții malefice care permit accesarea neautorizată a unui calculator, respectiv copierea fișierelor, și chiar controlarea comenzilor calculatorui penetrat.
- Caii troieni, care tehnic nu sunt viruși informatici, pot fi descărcați cu ușurință și în necunoștință de cauză. Spre exemplu, dacă un joc pe calculator este astfel proiectat ca la executarea sa de către un utilizator deschide o ușa de intrare (back door) pentru un hacker, care poate prelua ulterior controlul computerului, se spune despre acel joc că este un *cal troian*. Dacă în schimb, jocul este corect codat, dar a fost infectat ulterior cu un virus informatic, nu poate fi numit un *cal troian*, indiferent ce pagube poate produce virusul.

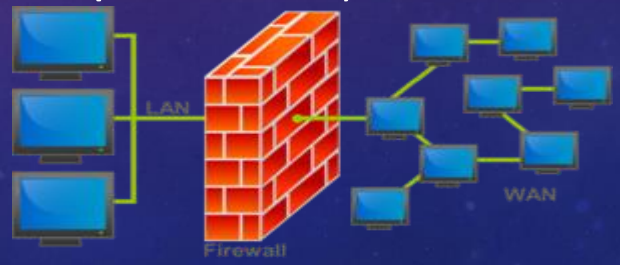
CAZURI NOTABILE ALE CAILOR TROIENI



- Cazuri notabile
- ***Back Orifice***
- ***NetBus***
- ***Zlob***
- ***Pest Trap***

FIRE-WALL – PARAVAN INFORMATIV

- În rețelele de calculatoare, un **firewall**, denumit și **paravan de protecți** (sau **parafoc**, în engleză *firewall*) este un dispozitiv sau o serie de dispozitive configurate în așa fel încât să filtreze, să cripteze sau să intermedieze traficul între diferite domenii de securitate pe baza unor reguli predefinite.
- Paravanele de protecție pot fi clasificate după:
- *- Un paravan de protecție poate ține la distanță traficul Internet cu intenții rele, de exemplu hackerii, viermii și anumite tipuri de viruși, înainte ca aceștia să pună probleme sistemului. În plus, un paravan de protecție poate împiedica participarea computerului la un atac împotriva altora, fără cunoștința sau voința utilizatorului. Utilizarea unui paravan de protecție este importantă în special dacă rețeaua sau computerul de protejat sunt conectate în permanență la Internet.



- Un paravan de protecție este o aplicație sau un echipament software care monitorizează și filtrează permanent transmisiile de date realizate între PC sau rețeaua locală și Internet, în scopul implementării unei "politici" (metode) de filtrare. Această politică poate însemna:
- protejarea resurselor rețelei de restul utilizatorilor din alte rețele similare, toate interconectate printr-o rețea de arie largă sau/și Internet. Posibilii atacatori sunt identificați, atacurile lor asupra PC-ului sau rețelei locale putând fi oprite.
- controlul resurselor la care au acces utilizatorii locali (din rețeaua locală).
- modul de implementare

SOFTWARE-UL RĂU INTENȚIONAT

- **Software-ul rău intenționat**, software dăunător, software nociv (numit adesea ***malware***, cuvânt englez pronunțat /ˈmælwɛər/, construit din sintagma ***mal****icious soft****ware***, „software răuvoitor”) este un tip de software proiectat intenționat pentru deteriorarea unui computer sau infiltrarea în el, sau/și deteriorarea ori infiltrarea în întregi rețele de computere, fără consimțământul proprietarului respectiv. Noțiunea se utilizează generalizat de către informaticieni pentru a desemna orice formă ostilă, intruzivă sau supărătoare de software sau cod de program.[6] Termenul de *virus* din domeniul computerelor este uneori utilizat pentru a desemna nu numai virușii informatici, ci și toate formele de software rău intenționat.

SCOPURILE ACESTUI SOFTWARE

- De cele mai multe ori,malware-ul este folosit pentru a lua,fară voia proprietarului,informații personale din computer-ul infectat,cum ar fi:
- Parole
- Date bancare
- Alte informații confidențiale

SPYWARE

- **Programele spion**[1] sau ***spyware*** (citit /'sp‿ai.wɛə/, din engleză *spy*/spionaj + *ware*/marfă) sunt o categorie de software rău intenționat, atașate de obicei la programe gratuite (jocuri, programe de schimbat fișiere, programe de chat pornografic, etc.), care captează pe ascuns date de marketing (prin analiza siturilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ș.a.m.d.) și le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.
- Programele spion care nu extrag date de marketing, ci doar transmit reclame se numesc *adware* (din engleză: *ad* = *advertising* = publicarea de reclame).
- Există programe spion care modifică modul de comportare a unor motoare de căutare (Google, Yahoo, MSN, etc.), pentru a trimite utilizatorul contra voinței sale la situri (scumpe) care plătesc comisioane producătorului programului spion.

- Unele programe spion abuzează de calculatorul utilizatorului pentru a face pe ascuns calcul distribuit (de exemplu operațiuni contabile pentru firme din India). SETI@home face tehnic același lucru, dar nu este considerat un program spion, deoarece face acest lucru numai cu consimțământul activ și explicit al utilizatorului. Din motivul că procesorul lucrează și pentru altcineva, programele spion încetinesc calculatorul [2]. Ele pot uneori să blocheze conexiunea la internet (ca efect neintenționat).
- În general, chiar după ștergerea programelor gratuite care au instalat programul spion, acesta rămâne în continuare activ. Există și numeroase programe anti-spion, dar atenție: unele dintre ele sunt *false antispyware* - inducând utilizatorul în eroare deoarece ele însele conțin programe spion mascate.

ADWARE

- **Adware** este orice program care afișează reclame la rularea acestuia, reclame care pot fi afișate ca bannere în fereastra programului, sau de tip pop-up (care deschide ferestre noi cu reclame, deasupra tuturor ferestrelor). Unele programe adware pot fi considerate o formă de spyware care nu colectează date de marketing, ci doar transmit reclame.Prin reclamele lui se poate sa iti colecteze date personale sau sa îți instaleze in dispozitiv viruşi.Dar unele aplicații tip Adware pot fi controlate de la distanta.

VIRUS TOTAL

- **VirusTotal** este un site web care oferă servicii gratuite de verificare a fișierelor contra virușilor. Acesta folosește până la 54[2] de producte antivirus diferite[3] și motoare de scanare pentru a verifica fișierele dacă sunt virusate sau pentru a verifica contra cazurilor *fals pozitiv*.[4] Fișierele de până la 128 MB pot fi încărcate pe site sau trimise prin email.[5] Producătorii de software anti-virus pot primi copii ale fișierelor depistate de alte scanere ca fiind infectate, dar omise de propriul product antivirus, pentru a-și îmbunătăți propriul lor software. De asemenea utilizatorii pot scana URL-uri suspecte și să caute prin *dataset*-ul VirusTotal. VirusTotal este un serviciu multilingvistic disponibil în peste 24 de limbi.
- VirusTotal a fost ales de către *PC World* drept unul din cele mai bune 100 produse ale anului 2007.[6]
- Pe 7 septembrie 2012 s-a anunțat faptul că Google Inc. a achiziționat VirusTotal.

SPAM

- **Spamming** (sau **spam** [spæm]) este procesul de expediere a mesajelor electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse și servicii dubioase, practicată în industria e-marketingului și de proprietarii de situri pornografice. *Spam*-ul se distinge prin caracterul agresiv, repetat și prin privarea de dreptul la opțiune.
- Această metodă se folosește și la colectarea adreselor de e-mail utilizând metode de genul *Citește și dă mai departe*. Conținutul acestor mesaje variază de la texte biblice, urări de bine cu îndemnarea de a trimite mai departe, în caz contrar vor urma evenimente neplăcute, până la mesaje cu caracter alarmant menite să atragă atenția asupra unui fapt plauzibil, îndemnând cititorul să trimită mesajul și altor persoane.

ANTIVIRUS

- **Software-ul antivirus** este folosit în general pentru prevenirea și eliminarea virușilor de computer, viermilor și cailor troieni. De asemenea, poate detecta și elimina adware, spyware și malware.
  Istorie[modificare | modificare sursă]
- Dr. Solomon's Anti-Virus Toolkit, AIDSTEST și AntiVir au fost lansate în 1988. La sfârșitul lui 1990 erau disponibile 19 produse antivirus, inclusiv Norton AntiVirus și McAfee VirusScan.
- Înainte de apariția Internetului, virușii s-au răspândit prin dischete, software-ul antivirus fiind actualizat relativ rar.

HACKER

- Un **hacker** este un expert în informatică, care se ocupă cu studiul în profunzime al programelor informatice (sisteme de operare, aplicații), adesea folosind tehnici de inginerie inversă (demontare), cu scopul de a obține cunoștințe care nu sunt accesibile publicului larg. Cei ce folosesc aceste cunoștințe în scopuri ilegale, pentru a compromite securitatea sistemelor informatice sau a aplicațiilor, sunt de fapt crackeri (spărgători), însă în percepția publicului (formată de obicei de mass-media) noțiunile de hacker și cracker adesea se confundă.

HACKERI RENUMIȚI

- Hackeri renumiți
- Richard Stallman este considerat un hacker și părintele mișcării pentru software liber.
- John Thomas Draper zis „Captain Crunch”, creator al cutiei albastre, instrument de phreaking.[9]
- Steve Wozniak zis „Woz”, co-fondator al Apple, a produs primul PC de succes.[9]
- Loyd Blankenship zis „The Mentor”, autor al Manifestului unui hacker, membru al grupurilor Extasyy Elite și Legion of Doom.
- Kevin Mitnick în trecut unul dintre hackerii cei mai căutați de către FBI, actualmente este consultant pe probleme de securitate și autor, nu are voie să atingă calculatoare, altfel va face din nou închisoare.[9]

- Eric Corley (cunoscut și ca Emmanuel Goldstein) pe numele său adevărat Eric Gorden Corley, parte a comunității hacker-ilor începînd cu sf. anilor 1970, este editorul revistei 2600:The Hacker Quarterly și unul din inițiatorul conferințelor H.O.P.E.
- Fyodor pe numele său adevărat Gordon Lyon, este autorul scanerului de securitate Nmap, cît și a mai multor cărți și pagini web axate pe probleme de securitate a rețelelor. Este membru fondator a Proiectului Honeynet și vice-președinte al Profesioniștilor din domeniul IT pentru Responsabilitate Socială.
- Solar Designer este pseudonimul fondatorului Proiectului Openwall.
- Michał Zalewski, cunoscut și ca „lcamtuf” este un recunoscut cercetător pe probleme de securitate informațională.
- Gary McKinnon este un hacker britanic care riscă să fie extrădat în SUA sub acuzația de spargere de rețele, ceea ce a fost descris ca „cea mai mare spargere a rețelelor militare din toate timpurile”.
- Julian Assange hacker fondator al Wikileaks.

PROGRAME ANTIVIRUS

- Produse de securitate[modificare | modificare sursă]
- O parte din aceste produse conțin pe lângă protecția antivirus și alte module precum antispam, firewall, control parental și lista poate continua.
- Ad-Aware Free Antivirus+/Ad-Aware Personal Security/Ad-Aware Pro Security/Ad-Aware Total Security, dezvoltate de Lavasoft (Germania)
- Avast Antivirus/Avast Internet Security/Avast Premier/Avast Pro Antivirus, dezvoltate de Avast (Cehia)
- Avetix Pro, dezvoltat de Avetix (Italia)
- AVG Antivirus/AVG PC TuneUp/AVG Internet Security, dezvoltate de AVG Tehnologies (Cehia)
- Avira Antivirus/Avira Internet Security, dezvoltate de Avira (Germania)

- BitDefender Antivirus Plus/BitDefender Internet Security/BitDefender Total Security, dezvoltate de Bitdefender (Ro)
- BullGuard Antivirus/BullGuard Internet Security, dezvoltate de BullGuard (UK)
- CA Anti-Virus, dezvoltat de CA Technologies (SUA)
- ClamWin, dezvoltat de ClamWin (Australia)
- F-Secure Antivirus/F-Secure Internet Security, dezvoltate de F-Secure (Finlanda)
- G Data Antivirus, dezvoltat de G Data Software (Germania)
- Immunet, dezvoltat de Cisco Sistems (SUA)

Kaspersky Anti-Virus/Kaspersky Internet Security, dezvoltate de Kaspersky Lab (Rusia)

- McAfee Antivirus/McAfee Internet Security, dezvoltate de McAfee [Intel Security] (SUA)
- Microsoft Security Essentials, dezvoltat de Microsoft (SUA)
- Norman Antivirus, dezvoltat de Norman Safeground
- Norton AntiVirus/Norton Antivirus Security, dezvoltate de Symantec (SUA)
- PSafe Total, dezvoltat de PSafe, (Brazilia)
- Qihoo 360 Total Security, dezvoltat de Qihoo 360 (China)
- Rising Antivirus, dezvoltat de Rising AntiVirus (China)

- SecureAnywhere AntiVirus/ SecureAnywhere Internet Security Plus, dezvoltate de Webroot (SUA)
- Trend Micro Antivirus+ Security, Trend Micro Internet Security, Trend Micro Maximum Security, Trend Micro Premium Security, Trend Micro Antivirus for Mac, dezvoltate de Trend Micro (Japonia)
- UnThreat Internet Security, dezvoltat de Scandium Security (Cipru)
- VirusBuster, dezvoltat de VirusBuster
- Windows Live OneCare, dezvoltat de Microsoft (SUA)
- Zemana Antilogger and Antimalware, dezvoltat de Zemana (Turcia)

PHISHING

- În domeniul securității calculatoarelor, **înșelăciunea**[1] (denumită în engleză ***phishing***, pronunțat /'fi-șin/) reprezintă o formă de activitate infracțională care constă în obținerea unor date confidențiale, cum ar fi date de acces pentru aplicații de tip bancar, aplicații de comerț electronic (ca eBay sau PayPal) sau informații referitoare la carduri de credit, folosind tehnici de manipulare a datelor identității unei persoane sau a unei instituții.
- O înșelăciune electronică constă, în mod obișnuit, în trimiterea de către atacator a unui mesaj electronic, folosind programe de mesagerie instantanee sau telefon, în care utilizatorul este sfătuit să-și dea datele confidențiale pentru a câștiga anumite premii, sau este informat că acestea sunt necesare datorită unor erori tehnice care au dus la pierderea datelor originale. În mesajul electronic este indicată de obicei și o adresă de web care conține o clonă a sitului web al instituției financiare sau de trading. Majoritatea *phisherilor* folosesc această metodă pentru a obține date bancare.
- Grupul de lucru antiînșelăciune (APWG), o organizație creată de către forțele de apărare a legii și organizații comerciale, raportează o creștere permanentă a acestui tip de atacuri.

MOTOARE ȘI DATASET-URI DE SCANARE A WEBSITE-URILOR/DOMENIILOR

- DMINUSLabs (ADMINUSLABS)
- AegisLab WebGuard (AegisLab)
- Alexa (Amazon)
- Avira Checkurl (Avira)
- BitDefender (BitDefender)
- CRDF (CRDF FRANCE)

- C-SIRT (Cyscon SIRT)
- CLEAN MX (CLEAN MX)
- Comodo Site Inspector (Comodo Group)
- CyberCrime (Xylitol)
- Dr.Web Link Scanner (Dr.Web)
- Emsisoft (Emsi Software GmbH)
- ESET (ESET)
- FortiGuard Web Filtering (Fortinet)

- G-Data (G Data)
- Google Safebrowsing (Google)
- K7AntiVirus (K7 Computing)
- Kaspersky URL advisor (Kaspersky Lab)
- Malwared (Malwared.ru)
- Malware Domain Blocklist (DNS-BH - Malware Domain Blocklist)

- Malware Domain List (Malware Domain List)
- MalwarePatrol (MalwarePatrol)
- Malwares.com (Saint Security)
- Netcraft (Netcraft)
- Opera (Opera)
- Palevo Tracker (Abuse.ch)
- ParetoLogic URL Clearing House (ParetoLogic)
- Phishtank (OpenDNS)
- Quttera (Quttera)

- SCUMWARE (Scumware.org)
- SecureBrain (SecureBrain)
- Sophos (Sophos)
- ThreatHive (The Malwarelab)
- Trend Micro Site Safety Center (Trend Micro)
- urlQuery (urlQuery.net)

- VX Vault (VX Vault)
- Websense ThreatSeeker (Websense)
- Webutation (Webutation)
- Wepawet (iseclab.org)
- Zeus Tracker (Abuse.ch)
- Zvelo (Zvelo)

CE PERICOLE TE PÂNDESC ÎN SPATELE CONTULUI DE FACEBOOK

- **facebook** (pronunțat /'feis.buk/ v. AFI) este un site web de tip rețea de socializare din Internet, creat de către Mark Zuckerberg în anul 2004 pentru a oferi posibilitatea de a contacta persoane apropiate, dar și persoane încă necunoscute. În acest moment facebook este una dintre cele mai răspândite rețele sociale din lume. Utilizatorii pot intra în această rețea din orice loc unde există acces la Internet pe baza unei parole, stabilite inițial odată cu completarea formularului de înscriere conținând o serie întreagă de întrebări personale. În prezent (noiembrie 2015) site-ul facebook are circa 1.44 mild. membri în toată lumea [4]. Apreciat a fi al doilea sit social mondial după google.com, luat după numărul de vizite, facebook face parte din fenomenul recent denumit Web 2.0. În februarie 2004 Mark Zuckerberg a fondat rețeaua „*The Facebook*”, având la început denumirea „thefacebook.com”. facebook, lansată inițial ca o rețea universitară, a fost extinsă apoi angajaților unor companii ca Apple și Microsoft.

- **A sparge un cont pe o reţea de socializare nu este o misiune imposibilă pentru un hacker. De aceea, trebuie să oferim cât mai puţine informaţii personale în mediul de comunicare on-line**

  Specialiştii atrag atenţia că principalele pericole care se ascund în spatele reţelelor de socializare, fie că vorbim depre Facebook, LinkedIn, Myspace, hi5 sau orice altă reţea similară, sunt create tocmai de disponibilitatea noastră de a împărtăşi informaţii personale. Potrivit lui Cătălin Cosoi, şeful Online Threats Lab al Bit- Defender, reţelele de socializare sunt nişte baze de date imense cu informaţii personale despre utilizatori, la care oricine are acces.

- "Acest lucru uşurează foarte mult sarcina unor persoane rău intenţionate, care practic nu trebuie decât să vină cu metodele potrivite de inginerie socială care să îi convingă pe utilizatori să dea click", a declarat acesta, pentru EVZ. Conform specialistului, acest lucru se întâmplă destul de frecvent, pentru că oamenii nu sunt pe deplin conştienţi de riscurile pe care le implică publicarea datelor personale pe internet. **Dependenţa de reţelele de socializare** Ai câteva sute bune de prieteni virtuali, sute de poze încărcate, şi zeci de comentarii urcate în fiecare zi? Ei bine, psihologii ar spune că ai o problemă. Dependenţa de internet, şi, în particular, cea de Facebook, a fost recunoscută de Asociaţia Americană de Psihiatrie. Potrivit psihologului Lena Rusti, pe reţelele de socializare vrem să ne arătăm lumii aşa cum nu suntem, respectiv siguri pe noi şi încrezători, şi să atragem atenţia.

- Aceasta este şi explicaţia pentru dezinhibarea de care dau dovadă multe dintre persoanele care utilizează aceste reţele de socializare. Reacţia primită din partea celorlalţi poate juca un rol important în inducerea unei stări de dependenţă de această formă de comunicare. Astfel că, în loc să stimuleze comunicarea, aceste reţele stimulează de fapt competiţia, spune psihologul. "Există şi avantaje, atâta timp cât aceste reţele te ajută să fii o fiinţă comunicaţională şi nu îţi apără incapacitatea de a comunica", a declarat Lena Rusti. **Metode de a sta departe de probleme** Potrivit specialiştilor, cei care divulgă prea multe informaţii personale pe reţelele de socializare se expun mai multor riscuri, printre care cel de furt al identităţii şi cel de a deveni o ţintă pentru agresorii sexuali.

- Specialiştii contactaţi de EVZ te sfătuiesc ca, înainte de a posta o fotografie sau un comentariu pe reţele de socializare, să te gândeşti dacă ai vrea ca o persoană străină, întâlnită pe stradă, să ştie ce gândeşti sau cum arăţi, de exemplu, în noul costum de baie. De asemenea, trebuie să fim conştienţi că nu s-a inventat un cont care să nu fie spart. Dacă nu vrei ca şeful să vadă cum te plângi prietenilor virtuali de job, atunci ar fi bine să te abţii să faci astfel de comentarii pe reţelele de socializare. Când alegi să postezi o fotografie, gândeşte-te bine dacă nu îţi va fi ruşine de ea peste câţiva ani sau dacă nu-ţi va afecta imaginea mai târziu, când un posibil angajator o va găsi pe internet.

- Deşi multe dintre reţele nu permit crearea unui cont pentru cei sub 13 ani, sunt destule persoane care postează fotografii în care copiii lor sunt goi sau sumar îmbrăcaţi, fără a realiza că în spatele prietenului virtual se poate afla un pedofil. **Cum să evităm riscurile de securitate** Scopul reţelelor de socializare este tocmai acela de a permite interacţiunea cu cât mai mulţi oameni din întreaga lume. "Decizia de a ascunde sau de a împărtăşi anumite informaţii rămâne în final a utilizatorului. El îşi configurează setările, el îşi alege prietenii virtuali, el alege ce informaţii să posteze.

SURSĂ

- http://www.evz.ro/ce-pericole-te-pandesc-in-spatele-contului-de-facebook-940381.html
- https://ro.wikipedia.org/wiki/Virus_informatic