COLEGIUL TEHNIC „VICTOR UNGUREANU”
CÂMPIA TURZII

PROIECT

PENTRU OBŢINEREA CERTIFICATULUI DE CALIFICARE
PROFESIONALĂ NIVEL 4

TEHNICIAN OPERATOR TEHNICĂ DE CALCUL

ABSOLVENT:
CHIRA V.D. DARIUS-CORNELIU

COORDONATOR:
prof. ARION LOREDANA

2019 – 2020

Clasificarea şi descrierea tipurilor de viruşi informatici

CONŢINUT

ARGUMENT

Stresul utilizatorilor de calculator pentru siguranţa datelor de pe hard discul propriu este motivat în principal de existenţa viruşilor. Aceştia pot compromite total informaţiile de pe disc sau pot cauza alte mici neplăceri. Însă termenul virus este utilizat abuziv cu sens generic pentru ca sunt situaţii când datele sunt atacate de alte creaţii diabolice. Concret, există mai mulţi termeni, fiecare specializat pe un anumit tip de atac, cu consecinţe, desigur, diferite faţă de ceilalţi membri ai familiei viruşilor.

În Dicţionarul de informatică, englez-român, realizat de un englez, S.M.H. Collin, virusul este definit ca fiind „un program care se ataşează singur unui fişier (de obicei executabil), de unde atacă alte fişiere din sistem, la care se ataşează de fiecare dată când fişierul infestat iniţial este rulat“; acelaşi termen este explicat şi în Mini dicţionarul explicativ de termeni informatici modern, realizat de Ion-Victor Papa: „viruşii reprezintă programe de dimensiuni mici, concepute de către anumiţi programatori maniaci şi nu numai, care nu mai au ce face. [...] nu toţi viruşii sunt făcuţi pentru a dauna calculatoarelor în mod esenţial, ci numai pentru a crea neplăceri utilizatorului, pentru ca acesta sa-şi iasă în final din minţi“.

Calul troian a călătorit prin istorie şi, mai mult, s-a multiplicat ajungând pe computere, fără să fie dorit de acestea. Deşi în unele publicaţii mai întâlnim denumirea din engleza, Trojan Horse, este absurd să o utilizam având corespondentul românesc. Dicţionarul de informatică, realizat de Collin defineşte troianul astfel: „program introdus într-un sistem de către un pirat informatic (hacker); programul deghizat sub forma unei aplicaţii inofensive are de fapt rolul de a copia informaţii păstrate în fişiere confidenţiale, pe care piratul le poate accesa, astfel, fără autorizaţia proprietarului“.

Un alt cuvânt din familia celor deja expuse este vierme. El nu se regăseşte în dicţionarele de informatică, însă resursele de pe Internet l-au înregistrat de ceva vreme. Un dicţionar on-line redactat de către Guy Brand şi Jean-Pierre Kuypers defineşte simplu viermele ca fiind „un mic program autonom care infectează“.

Aceştia sunt principalii termeni cu care operăm atunci când ne referim la pericolele care ne pot afecta computerul. Cum ne ferim de aceste pericole? Prin precauţie în navigarea pe Internet şi în deschiderea unor fişiere necunoscute. O altă soluţie este instalarea unui soft antivirus.

I. DEFINITIA VIRUŞILOR

Ce este un virus de calculator?

Un virus este un program capabil de a se înmulţi, strecurându-se printre programele de pe un calculator sau dintr-o reţea şi provocând diverse efecte, de la unele inofensive, până la unele distructive.

În domeniul informatic se utilizează termenul virus din cauza asemănărilor funcţionale dintre aceste bucăţi de cod (programe) şi vieţuitoarele microbiologice.

O definiţie ceva mai academică, spune că virusul este de fapt un acronim, provenit de la **Vital Information Resources Under Siege**.

Viruşii se împrăştie ataşându-se de alte programe, fişiere EXE sau COM, iar mai recent, şi documentelor WORD, EXCEL, chiar şi fişierelor HLP, sau unii pot să infecteze sectorul de boot al discului. Când se lansează în execuţie un fişier infectat, sau când se porneşte calculatorul de pe un disc sau o dischetă virusată, se lansează şi virusul în execuţie. Adesea, virusul rămâne rezident în memoria calculatorului, pentru a putea infecta următorul program lansat în execuţie, sau următoarea dischetă accesată.

Ceea ce fac viruşii periculoşi este abilitatea lor de a executa acţiuni în calculator. În timp ce unele din aceste acţiuni sunt sâcâitoare (cum ar fi afişarea unui mesaj la o anumită dată sau ca răspuns la o anumită acţiune a utilizatorului calculatorului) iar altele enervante (cum ar fi reducerea performanţelor calculatorului), există viruşi care pot provoca adevărate catastrofe, distrugând fişiere de date, documente, sau făcând calculatorul inutilizabil.

Primii viruşi au apărut acum câteva decenii, însă nu au cunoscut o răspândire la scară mondială decât după apariţia primelor PC-uri. În 1981 firma IBM scotea pe piaţă, alături de gigantele mainframe-uri care îi aduseseră succesul, un calculator "personal" bazat pe noul (pe atunci) procesor produs de firma Intel, 8088. Preţul acestuia era extrem de ridicat, însă produsul a fost un succes. Ca sistem de operare IBM a cumpărat MS-DOS de la firma Microsoft, care la rândul ei l-a scris pe baza sistemului de operare CP/M. Primele versiuni de DOS erau extrem de compacte (numai câteva zeci de Kb) şi nu aveau nici un protocol de securitate inclus.

Trec 5 ani şi ajungem în 1986 când apăreau primele rapoarte publice indicând entităţi virale pe IBM-PC. Era vorba de virusul Brain, un virus de boot. Apar astfel programe de tip antivirus create

pentru a elimina viruşii informatici. Dacă primele programe antivirus erau extrem de simple, ca şi viruşii de pe atunci, programele din ziua de astăzi sunt adevărate "capodopere" de algoritmi şi cod.

Cum se răspândesc viruşii?

Viruşii pot proveni dintr-o varietate de surse. Pentru că un virus reprezintă cod executabil, el poate fi transmis pe toate căile normale de transmitere a informaţiei între calculatoare.

Într-un studiu din 1991 al companiei Dataquest realizat la cererea National Computer Security Association din Statele Unite, cel mai des viruşii se transmiteau prin dischete infectate (87 %). 43% din dischetele infectate, responsabile pentru introducerea viruşilor pe calculatoarele întreprinderilor erau dischete aduse de acasă. Aproape trei sferturi (71%) din infecţii au apărut în întreprinderi cu reţele de calculatoare, crescând pagubele prin rapida împrăştiere a viruşilor în toată reţeaua. În mediile de reţea, riscul infectării cu viruşi este mult crescut. Alte surse de dischete infectate erau dischetele demo sau conţinând software arhivat - circa 6% din infecţiile raportate.

La ora actuală, una din cele mai frecvente metode de răspândire a aplicaţiilor maliţioase este prin e-mail. Unele programe de e-mail protejează mesajele şi calculatorul prin blocarea automată a accesului la ataşamentele nesigure, precum şi prin filtrarea e-mail-urilor.

Deseori utilizatorul este păcălit să deschidă fişierul ataşat printr-un text din subiectul e-mail-ului sau printr-un titlu interesant al ataşamentului, cum ar fi o imagine sau un document.

În prezent, un calculator cu care cineva se conectează la internet, şi care nu este dotat cu firewall, poate fi infectat cu viruşi în doar câteva secunde. Nici măcar nu este necesar ca utilizatorul să viziteze vreun site - calculatorul poate fi infectat prin simpla conectare la internet, prin atacuri aleatoare asupra adreselor de IP.

Ce pot face viruşii?

Aşa cum am spus şi mai devreme, unii viruşi sunt enervanţi, iar alţii pot fi deosebit de periculoşi. În cazul cel mai fericit, viruşii cresc dimensiunea fişierelor şi reduc viteza de răspuns, afectând performanţele calculatorului nostru. Mulţi viruşi caută doar să se răspândească, nu să afecteze calculatorul, astfel încât nu produc daune în mod intenţionat. Totuşi, există posibilitatea ca şi viruşi benigni să interacţioneze întâmplător cu alte programe sau chiar cu hardware-ul şi să încetinească sau să oprească sistemul. Alţi viruşi sunt mult mai periculoşi. Aceştia pot modifica sau distruge datele, sau pot şterge fişierele şi pot reformata hard-discul.

Care sunt simptomele unui sistem virusat?

Cei care sunt iniţiaţi în domeniul viruşilor de calculatoare nu vor avea probabil dificultăţi în a spune dacă un calculator este suspect de a fi infectat cu un virus nou. Viruşii se pot răspândi

nestingheriţi doar atâta timp cât rămân nedetectaţi. Din acest motiv, majoritatea viruşilor nu îşi manifestă prezenţa în sistem. Numai programele antivirus pot detecta prezenţa unei asemenea infecţii. Există, totuşi, mai mulţi viruşi, ce îşi fac simţită prezenţa în sistem prin efectele secundare generate.

Câteva "simptome" specifice calculatoarelor virusate (lista este orientativă, cazurile reale fiind mult mai numeroase şi diverse):

- fişierele sistem cresc în lungime (de exemplu în DOS 6.20 fişierul command.com are 54619 octeţi, iar pe un calculator virusat el poate avea, să zicem cu 1200 de octeţi mai mult, respectiv 55819);
- blocări frecvente - majoritatea viruşilor sunt extrem de prost scrişi şi blochează calculatorul extrem de des. Viruşii sunt de altfel cunoscuţi ca cele mai incompatibile programe (exceptând viruşii multiplatforma, ca de exemplu clasa "Concept" - viruşii de .doc Word);
- mesaje ciudate, melodii sau sunete suspecte în difuzor. Mulţi viruşi îşi fac anunţată prezenţa prin astfel de efecte;
- distrugerile de date sunt alt efect al viruşilor. Dispariţia subită a unui fişier sau erori ale sistemului de fişiere sunt clasice;
- încetinirea accesului la disc este produs de unii viruşi stealth care se interpun între programe şi sistemul de acces la discuri;
- la apăsarea tastelor CTRL+ALT+DEL calculatorul bootează instantaneu fără a mai trece prin ecranul de POST (power on, self test);
- la comanda chkdsk majoritatea programelor executabile sunt raportate ca având o lungime incorectă: efect al unor viruşi stealth;
- dimensiunea memoriei afişată de programele specializate este mai mică decât 640Kb. Uneori acest efect este generat de unele managere de memorie fără a fi vorba de un virus, dar de obicei indică prezenţa unui virus;
- programele de tip self-check raportează că au fost modificate;
- nu mai porneşte Windows sau se raportează că accesul la disc se face prin BIOS;
- schimbări ale marcajului de timp al fişierelor;
- încărcarea mai grea a programelor;
- operarea înceată a calculatorului;
- sectoare defecte pe unităţi de memorie externă.

II. CLASIFICAREA VIRUŞILOR

O clasificare riguroasa nu există încă,dar se poate face ţinând seama de anumite criterii.

În forma cea mai generală viruşii se împart in:

- Viruşi hardware
- Viruşi software

Viruşii hardware sunt mai rar întâlniţi,aceştia fiind de regulă, livraţi o dată cu echipamentul. Majoritatea sunt viruşi software, creaţi de specialişti în informatică foarte abili şi buni cunoscători ai sistemelor de calcul, în special al modului cum lucrează software-ul de bază şi cel aplicativ.

Din punct de vedere al capacitaţii de multiplicare, viruşii se împart în două categorii:

- Viruşi care se reproduc, infectează şi distrug
- Viruşi care nu se reproduc, dar se înfiltrează în sistem si provoacă distrugeri lente, fără să lase urme (Worms).

În funcţie de tipul distrugerilor în sistem se disting:

- Viruşi care provoacă distrugerea programului în care sunt incluşi
- Viruşi care nu provoacă distrugeri, dar incomodează lucrul cu sistemul de calcul; se manifestă prin încetinirea vitezei de lucru,blocarea tastaturii,reiniţializarea aleatorie a sistemului, afişarea unor mesaje sau imagini nejustificate
- Viruşi cu mare putere de distrugere,care provoacă incidente pentru întreg sistemul, cum ar fi: distrugerea tabelei de alocare a fişierelor de pe hard disk, modificarea conţinutului directorului rădăcină, alterarea integrală şi irecuperabilă a informaţiei existente

Programele virus se mai împart în două categorii mari:

- Viruşi nedistructivi
- Viruşi distructivi

Printre viruşii nedistructivi cele mai mari categorii sunt:

- *Viermi* (Worms): Este o categorie de viruşi, care au capacitatea de a infecta calculatoarele în special prin reţeaua Internet. De obicei ei folosesc calculatorul gazdă pentru a ataca anumite site-uri web, sau funcţionează la fel ca şi viruşii tip *Cal Troian*.
- *Spioni* (Spyware): Programele spion se instalează pe calculatorul tău fără ca să ştii ceva despre aceasta. Ele colectează informaţiile tale personale, stocate pe calculator şi te fac vulnerabil la infracţiunile de furt de identitate. Tot spionii pot

urmări care sunt site-urile, pe care le vizitezi în timp ce cauţi informaţii. Programele spion se descarcă pe calculatorul tău în timpul navigării pe Internet, în timpul accesării paginilor infectate sau dacă descarci fişiere neverificate ori citeşti mesaje de email nesolicitate.

- *Viruşi Adware:* Lansează pagini nedorite pe calculatorul tău în timpul navigării pe web. Pot încetini lucrul calculatorului sau chiar ă-l pot bloca.
- *Keylogger:* Programe care memorează fiecare şir de simboluri semnificativ (cheie) pe care î-l ai pe calculator. Astfel keyloggerii îţi fură codurile de acces, parolele şi datele personale.
- *Răpitori* (Browser hijackers): Programe mici care îţi pot schimba pagina de start a programului de explorare sau rezultatele căutărilor pe web.
- *Cal Troian* (Trojan horse): Aceşti viruşi se mai numesc *troiani teleghidaţi* sau RAT şi permit atacatorului să controleze calculatorul tău la distanţă, prin reţea.

Viruşii destructivi se împart şi ei în câteva grupe, după acţiunea pe care o exercită şi zona de memorie, pe care o atacă:

- *Viruşi a sectoarelor de încărcare* (boot sectors): Infectează programele de pe sectoarele de încărcare a dispozitivelor de stocare: dischete, harddisk, etc. În rezultat este deteriorat procesul de încărcare a sistemului de operare – calculatorul nu mai funcţionează.
- *Viruşi de fişiere* (File viruses): Aceşti viruşi pătrund în corpul programelor de aplicaţii şi se maschează în interiorul lor. Atunci când încerci să porneşti programul de aplicaţie infectat, se lansează virusul, care produce diferite daune calculatorului. Aplicaţia însă nu mai poate funcţiona, până nu este reinstalată sau lecuită cu un program antivirus.
- *Viruşi de extindere* (Extending viruses): Un virus care a pătruns în sistem se poate comporta ca un parazit. El se anexează la diferite fişiere, fie la sfârşit, fie la început, şi repetă aceasta ori de cîte ori apare o ocazie potrivită. În scurt timp vei observa că nu îţi mai ajunge memorie, iar tot mai multe aplicaţii refuză să se mai lanseze.
- *Viruşi de companie* (Companion viruses): Dacă ai fost atacat de un virus de companie, vei observa foarte repede acest lucru: fişierele tale încep să fie însoţite de arhive cu acelaşi nume, sau de fişiere executabile, care dublează numele

fişierelor de date. Atunci cînd apelezi un fişier, mai întîi este activat fişiereul executabil cu acelaşi nume, care conţine virusul. Acesta din urmă începe imediat activitatea sa destructivă.

- *Viruşi bacteriofagi:* Au fost numiţi astfel, deoarece sunt foarte agresivi, fa fel ca viruşii reali, care distrug bacteriile. Viruşii de calculator care fac parte din această categorie înlocuiesc codul programului din fişierele de pe calculator cu codul lor propriu. Un fişier infectat cu un virus bacteriofag nu mai poate fi lecuit. Asemenea fişiere pot fi doar lichidate sau supuse unei carantine.
- *Viruşi de cavitate:* Viruşii care se anexează altor programe de obicei fac aceasta fie la începutul codului program, fie la sfârşit. Aceasta face că dimensiunea fişierului să se modifice, ceea ce serveşte ca indiciu că fişierul este infectat. Din nefericire, există o categorie de viruşi, care îşi implantează codul în interiorul fişierelor executabile, folosind cavităţi ale codului executabil al programelor. Fişierele infectate nu îşi schimbă dimensiunea, îşi păstrează funcţionalitatea, dar poartă în sine programul virus, care se va activa neapărat la apariţia unei anumite situaţii (dată calendaristică, interval de timp de la infectare etc.)

III. ISTORIC VIRUŞI

1949

Sunt puse pentru prima oară bazele teoriilor legate de programele care se autoreproduc.

1981

Viruşii Apple 1, 2, si 3 sunt printre primii viruşi "in the wild". Descoperiţi in sistemul de operare Apple II, viruşii se răspândesc in Texas A&M prin intermediul jocurilor piratate.

1983

În teza sa de doctorat, Fred Cohen defineşte pentru prima oara formal un virus de calculator ca fiind "un program ce poate afecta alte programe de calculator, modificându-le într-un mod care presupune abordarea unor copii evoluate ale lor."

1986

Doi programatori, Basit şi Amjad, înlocuiesc 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 etichetă de disc (volume label).

1988

Scapă din lesă unul dintre cei mai cunoscuţi viruşi: J*erusalem*. Activat in fiecare vineri 13, virusul afectează fişierele .exe si .com si şterge toate programele rulate in cursul acelei zile.

1990

Symantec lansează pe piaţă Norton AntiVirus, unul dintre primele programe antivirus dezvoltate de către una dintre marile companii.

1991

Tequila este primul virus polimorf cu răspândire pe scara largă găsit "in the wild". Viruşii polimorfi fac ca detectarea lor de către scanerele de viruşi să fie dificilă, prin schimbarea modul de acţiune cu fiecare nouă infecţie.

1992

Există 1300 de viruşi, cu aproape 420% mai mulţi decât in decembrie 1990. Previziunile sumbre ale virusului *Michelangelo* ameninţă colapsul a circa 5 milioane de calculatoare pe data de 6 martie. Însă doar 5,000-10,000 de calculatoare se întâmplă să "dea coltul".

1994

Farsa de proporţii din partea email-ului hoax (alarmă falsă) *Good Times*. Farsa se bazează pe ameninţarea unui virus sofisticat care e capabil să şteargă un intreg hard prin simpla deschidere a

emailului al cărui subiect este "Good Times". Deşi se ştie despre ce e vorba, hoaxul revine la un interval de 6-12 luni.

1995

W*ord Concept*, virus de Microsoft Word, devine unul dintre cei mai răspândiţi viruşi din anii '90.

1998

StrangeBrew, actualmente inofensiv si totuşi raportat, este primul virus care infecteaza fişierele Java. Virusul modifică fişierele CLASS adaugând la mijlocul acestora o copie a sa si începând executarea programului din interiorul secţiunii virusate.

Virusul C*ernobîl* se răspândeşte rapid prin intermediul fişierelor ".exe". Dupa cum o sugerează si notorietatea numelui sau, virusul este nemilos, atacând nu numai fişierele dar şi un anumit cip din interiorul computerelor infectate.

1999

Virusul *Melissa*, W97M/Melissa, execută un macro dintr-un document ataşat emailului, care transmite mai departe documentul la 50 de adrese existente în Outlook address book. Virusul infecteaza si documente Word pe care le trimite ca ataşamente. Melissa se împrăştie mult mai rapid decat alti viruşi anteriori infectând cam 1 milion de calculatoare.

Bubble Boy este primul virus care nu mai depinde de deschiderea ataşamentului pentru a se executa. De îndată ce userul deschide email-ul, Bubble Boy se si pune pe treabă.

2000

Love Bug, cunoscut şi sub numele de „*I LOVE YOU"* se răspândeşte asemănător cu modul de răspândire al Melissei. Acest virus e primit ca un ataşament .VBS, şterge fişiere, inclusiv MP3, MP2 şi JPG şi trimite username-uri şi parole găsite în sistem autorului virusului. *W97M.Resume.A*, o noua varianta a Melissei, este "in the wild". Virusul se comportă cam ca Melissa, folosindu-se de un macro Word pentru a infecta Outlook-ul şi pentru a se răspândi. Virusul *Stages* deghizat intr-un email gluma despre etapele vieţii, se răspândeşte prin Internet. Deloc specific celorlalţi viruşi anteriori, Stages este ascuns intr-un ataşament cu extensie falsa .txt, momind utilizatorii să-l deschidă. Pană la apariţia sa, fişierele text erau considerate fişiere sigure.

2001

Nimda (2001) a fost un worm destinat să infecteze serverele, încetinind considerabil traficul pe internet. Una dintre caracteristicile sale cele mai frapante a fost viteza foarte mare cu care se răspândea, iar faptul că infecta serverele a determinat colapsul unor reţele de computere.

2003

SQL Slammer/Sapphire, un virus al serverelor, a provocat, în 2003, pagube estimate la 1 miliard USD; a fost vorba despre evenimente precum căderea serviciului de bancomat al Bank of America, probleme cu serviciul de apeluri de urgenţă 911 în Seattle, erori în sistemul de emitere a biletelor de avion electronice şi, în consecinţă, anularea unor zboruri - efecte care arată cât de grave pot fi urmările unui atac de malware în lumea contemporană, masiv informatizată.

2006

Storm Worm (cunoscut şi sub numele de Nuwar) a debutat în 2006; este un troian care permite controlul de la distanţă al computerelor de către crackeri, care le folosesc, de pildă, transformându-le în "fabrici de spam". A cam speriat lumea internetului prin amploarea atacului dar, deşi cu o răspândire foarte largă, s-a dovedit, din fericire, relativ uşor de îndepărtat, cu ajutorul unor programe anti-virus obişnuite.

2009

Viermele **Koobface** fură ID-uri şi liste de contacte de pe FaceBook, Twitter, MySpace, YouTube, Friendster şi Bebo.

2010

Stuxnet - Se crede că Stuxnet a fost dezvoltat, în timpul administraţiei Bush, de SUA şi Israel cu scopul de a combate programul nuclear iranian. Programul a fost conceput pentru a se şterge singur în 2012. Stuxnet, care a exploatat vulnerabilităţi din sistemul de operare Windows şi programul Step7 de la Siemens, ţintea în special computere din facilităţi industriale.

2016

Locky - Au existat peste 60 de versiuni ale acestui program dăunător, care au infectat câteva milioane de computere, majoritatea în Europa. La un moment dat în fiecare oră erau infectate aproximativ 5.000 de computere pe oră doar în Germania. Nici programele avansate de securitate actualizate la zi nu erau capabile să-i protejeze pe utilizatori de primele versiuni ale Locky.

2017

Wanna Cry este un program dăunător care criptează datele utilizatorilor şi apoi solicită recompensă. În timp ce ransomware-ul convenţional, una dintre cele mai prolifice ameninţări ale momentului, se răspândeşte prin emailuri cu documente periculoase ataşate, browser-e şi exploit-uri în aplicaţiile web, atacul de acum foloseşte o vulnerabilitate prezentă în majoritatea versiunilor sistemului de operare Windows.

IV. TOPUL CELOR MAI PERICULOŞI VIRUŞI

Părerile experţilor diferă în funcţie de anumite caracteristici, când vine vorba despre un astfel de clasament.

În ultimii 20 de ani, mii - dacă nu sute de mii - de viruşi au atacat calculatoarele utilizatorilor de pe mapamond. Alături de creatorii de soluţii de securitate, „Evenimentul zilei” a încercat să facă un top al celor mai periculoşi.

„Dacă ne întoarcem în anii ’90, putem spune că, probabil, cea mai semnificativă ameninţare informatică de la începutul acelor ani a fost virusul Cascade, care infecta sistemele DOS”, ne-a declarat Andrey Slobodyanik, director Kaspersky Lab Europa de Est.

Acesta era un virus criptat, pe care oamenii îl răspândiseră foarte mult. Însă, în acea perioadă, viruşii reuşeau să infecteze un număr ridicat de computere pe parcursul mai multor luni, nu foarte rapid ca acum. La mijlocul anilor ’90 am început să vedem macroviruşii, care se răspândeau pe durata a câtorva săptămâni, deci mult mai rapid. Aceştia infectau datele de pe computer, deoarece e-mailul devenise popular, iar oamenii îşi trimiteau mesaje cu diferite documente ataşate.

Apocalipsa digitală

Tot în perioada anilor ’90 au apărut „Melissa” sau „Love Letter”, care s-au răspândit automat, producând o „epidemie”. Potrivit unui studiu BitDefender, în ultimele zile ale anului 1999 apăruseră deja zvonuri despre un atac masiv ce urma să vină dinspre comunităţile creatorilor de viruşi, care ar fi urmat să infecteze într-un timp foarte scurt toate calculatoarele de pe mapamond. Mişcarea ar fi urmat să dezlănţuie apocalipsa digitală.

Începutul anilor 2000 a însemnat, de fapt, adevărata naştere a infracţionalităţii pe internet, deoarece, până în 2002, curentul era unul de cyber-vandalism. „Viruşii erau creaţi pentru a şterge date, a opri servere etc. Însă, anul 2003 a produs o schimbare esenţială - creatorii de viruşi şi-au spus «Toată lumea face tranzacţii financiare on-line, de ce să nu profităm de acest lucru? Putem să distribuim spam, să furăm datele de autentificare »", ne-a spus Vasily Dyagilev, director de vânzări în cadrul Kaspersky Labs.

Acesta a fost începutul cyber-criminalităţii. Au fost creaţi viruşi precum „Code Red" sau „Nimda", care se răspândeau rapid. În acelaşi timp, în 2001 a început şi exploatarea vulnerabilităţilor software. Cei de BitDefender spun că 2005 a fost anul în care viruşii pentru diferite platforme de mesagerie instantă şi-au pus serios amprenta.

La începutul acestui an, Win32.Worm.Prolaco.G s-a remarcat prin capabilitatea lui de infectare multiplă. Pentru 2010 şi viitorul apropiat, oficialii BitDefender cred că din cauza evoluţiei tehnologiei ce este mai periculos de abia acum va apărea.

Virus prin Yahoo Messenger: "Se extinde ca un foc de pădure"

Un mesaj instant care conţine un link foto, care pare a fi de la o persoană din lista ta de contacte, este noua variantă, agresivă, a unui virus mai vechi care se răspândeşte prin Yahoo Messenger şi permite atacatorului să preia controlul asupra computerului tău.

"Se extinde ca un foc de pădure", a spus Cătălin Cosoi, de la BitDefender. El a spus că virusul prin Yahoo Messenger a infectat numeroase calculatoare româneşti după 1 Mai. "Oamenii aşteaptă să vadă poze de la prieteni, colegi, după o zi de sărbătoare", spune Cosoi. Crezând că un prieten îi trimite poze, utilizatorul de Yahoo Messenger accesează link-ul. Virusul ar putea infecta şi calculatoarele din străinătate, spune specialistul român. După ce a infectat computerul tău, întreaga

listă de prieteni va primi acelaşi link. Acest virus este cunoscut ca Palevo (de Bitdefender), W32. Ymfocard.fam.Botnet (de BKIS) şi W32.Yimfoca (de Symantec).

Link-ul este asemănător unuia spre un fişier JPG, GIF sau PHP. Dar utilizatorul poate controla situaţia. În fapt, link-ul duce spre un fişier .exe, iar dacă utilizatorul nu îl rulează, virusul nu afectează calculatorul. Potrivit Symantec, dacă fişierul acesta este rulat, el se adaugă listei Windows Firewall şi opreşte serviciul Windows Update. Mai departe, uşor de înţeles, răufăcătorii preiau controlul computerului şi pot face absolut orice, de la furat parole la şters fişiere. "Natura atacului nu este nouă, deoarece această cale de atac a fost folosită anterior de alţi viruşi. Totuşi, este foarte periculoasă pentru utilizatori", spun şi cei de la BKIS.

Melissa. A apărut în 1999. A reușit să blocheze complet, pentru o perioadă scurtă, serverele de e-mail ale celor de la Intel și de la Microsoft. S-a transmis prin e-mail și era atașat într-un document ce părea că vine de la un prieten. David Smith, creatorul, a fost condamnat de justiția americană la 10 ani de închisoare și a primit o amendă de 5.000 de dolari. A fost eliberat după un an.

Mydoom. A fost creat de un rus în anul 2004 și s-a transmis tot prin e-mail. În mesaj scria că ai probleme de securitate cu adresa ta și te invita să accesezi un fișier. În documentul respectiv era virusul care îți infecta computerul, iar PC-ul devenea sursă pentru trimiterea mesajelor de tip spam.

Storm Worm. A apărut în anul 2007 și a reușit să afecteze în scurt timp peste 50 de milioane de computere din întreaga lume. Computerele infectate cu acest virus a reușit să trimită mesaje de tip spam până în urmă cu aproximativ trei ani. Era foarte greu de detectat pentru că își schimbă forma după aproximativ 30 de minute.

Contificker. Apărut în anul 2008. Acest virus este un purtător de alte infecții cibernetice și era plasat de hackeri în funcție de interesul lor, pe anumite domenii. Reușește să-ți dezactiveze antivirusul și blochează update-urile la sistemul de operare. Poate ajunge în computer prin intermediul memory stick-urilor infectate. Printre altele, a reușit să blocheze rețelele online ale Ministerului Apărării britanic și pe ale poliției norvegiene.

I love you. Creat în Statele Unite în anul 2000, acest virus a infectat milioane de PC-uri într-o singură noapte. A fost conceput de un student care a încercat să obțină niște parole ale unor

conturi. Până când s-a descoperit un antidot, virusul a reușit să provoace o pagubă de aproximativ 10 miliarde de dolari în întreaga lume.

Stuxnet. A fost descoperit în 2010 și se consideră că stă la baza unui atac cibernetic asupra rețelei de computere din cadrul programului nuclear iranian. De asemenea, sunt zvonuri că acest virus ar fi fost creat de specialiști ai serviciilor secrete din Statele Unite și Israel. Virusul a reușit să infecteze aproximativ 60% din computerele iranienilor și ar fi regresat sistemul nuclear al țării cu aproximativ doi ani.

Flamer. Și acest virus a fost descoperit în anul 2010 și acționează de pe memory stick-uri infectate. Este construit pentru a culege date de pe computere și rețelele care nu sunt conectate la internet. Imediat ce memory stick-ul este băgat într-un alt computer care are conexiune la internet, automat toate datele colectate sunt trimise către o adresă. Și despre acest virus se spune că ar fi creat tot de servicii secrete.

V. MĂSURI DE PREVENIRE ÎMPOTRIVA VIRUŞILOR

Utilizatorul, fie că este pe staţie individuală sau pe reţea, trebuie să ia toate măsurile pentru a preveni fenomenul de instalare a viruşilor. În acest scop acţiunile utilizatorului se împart în două categorii.

- măsuri de prevenire;
- măsuri de eliminare.

Măsurile de prevenire se referă în mod deosebit la:

1. Instalarea şi operarea numai cu software originale, achiziţionate de la firme producătoare sau dealeri autorizaţi. *"Pirateria"* software poate avea consecinţe dezastruoase, oferind în schimbul unui preţ redus de achiziţionare, viruşi cu efecte distructive nebănuite.
2. Limitarea numărului de utilizatori atât la staţiile individuale cât şi în reţelele de calculatoare (cu excepţia reţelelor publice). Aceasta se poate face atât prin sistemul *"password"* (parola) cât şi prin folosirea codurilor personale de acces, îndeosebi în reţelele de calculatoare.
3. Interzicerea sau limitarea instalării de jocuri în reţelele de calculatoare. La staţiile individuale aceasta depinde de utilizatorul-proprietar, în acest caz este de preferat achiziţionarea acelor jocuri distribuite în reţeaua de comercializare autorizată.

4. Păstrarea în original a programelor cele mai importante de preferat pe CD-uri ori pe dischete protejate la scriere, care să poată înlocui la nevoie pe cele virusate.

5. Realizarea periodica de copii *"backup"* pentru cele mai importante programe şi fişiere.

6. Crearea şi păstrarea protejata a unei dischete, ca disc sistem, astfel sa puteţi la nevoie încarcă sistemul de operare nealterat, fapt esenţial în acţiunea de devirusare.

7. Interzicerea utilizării (citirii) discurilor flexibile necunoscute. Aceasta se poate face numai după operaţiunea de scanare.

8. În caz de infestare cu un program virus, este obligaţia utilizatorului să avertizeze despre acest lucru pe toţi cei cu care a făcut schimb de software în ultima perioadă şi să întrerupă transferul de fişiere către alţi utilizatori.

9. Scanarea, care se aplică preventiv la preluarea fişierelor din afara sistemului şi este foarte utilă în faza primară de răspândire a viruşilor. Se recomandă ca operaţiunea de scanare să se efectueze periodic asupra fişierelor de pe hard disk.

10. Instalarea rezidentă a componentei de tip *"GUARD"* a programelor antivirus care să execute o căutare a viruşilor (scanare) atunci când:

- **a)** se iniţializează sistemul de operare;
- **b)** se citeşte unul din discurile memoriei externe (hard disk, CD, DVD);
- **c)** se lansează în execuţie un program.

11. Aplicarea unei măsuri antivirus de tip hardware. Aceasta constă dintr-o placă care conţine într-un EPROM (memorie ROM reprogramabilă) programele soft ce se lansează în procesul de iniţializare a calculatorului. Astfel, nici un virus nu poate deveni rezident în memorie înainte ca programele de verificare să îşi facă datoria, realizând o protecţie sigură. Dezavantajul, căci există un dezavantaj, constă în timpul mare angrenat într-o astfel de verificare.

Măsurile si acţiunile de eliminare a viruşilor se bazează pe folosirea unui program antivirus în actualitate cu ajutorul căruia să se execute o căutare (scanare) şi ulterior o eliminare (clean).

BIBLIOGRAFIE

- Dabija George, *Securitatea sistemelor de calcul***,** auxiliar curricular elaborat în cadrul proiectului *Învăţământul profesional şi tehnic în domeniul TIC,* proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013
- Dumitru, George *Programe Antivirus* Ed. Teora 1997
- Victor Valeriu Patriciu *Criptorafia şi securitatea reţelelor de calculatoare* Ed. Tehnică 1994 Bucureşti
- Peter Norton *Reţele de calculatoare* Ed. Teora 2002 Bucureşti
- Pagini Web:

  www.symantec.com
  www.microsoft.com