Spam
Keylogger
Spyware
E-mailurile de tip phishing

Proiect realizat de

Postovanu Iulian, Eni Alexandru, clasa XII-a C

Spam
Ce este spam-ul?

Spamming (sau **spam**) este procesul de expediere a mesajelor electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse și servicii dubioase. ***Spam***-ul se distinge prin caracterul agresiv, repetat și prin privarea de dreptul la opțiune.Orice mesaj in special nesolicitat și repetitive poate fi catalogat drept –spam.

Care sunt principalele canale de raspândire amesajelor de tip spam?

- E-mailul
- Comentariile
- Mesajele pe forumuri
- Rețelele de socializare (Facebook, Twitter, Instagram)
- Spamul prin SMS

Care sunt pericolele la care sunt expusi utilizatoriicând deschid astfel de mesaje?

- Primul este reprezentat de **mesajele de tip phishing**. Acestea pot fi extrem de daunatoare, pentru ca ele pretind a veni din partea unei institutii(uneori bancare, uneori nu).
- Cel de-al doilea pericol care există este **infectarea calculatorului prin deschiderea unui link periculos** dintr-un spam, prin download-ul si rularea unui executabil, prin deschiderea unui eventual atasament infectat etc. Dupa infectarea calculatorului, pericolele pot sa capete forme variate in functiede tipul de malware(Un program malware se refera la aplicatiile software sau secvente de cod executabile create special pentru a efectua operatii care afecteaza calculatorul prin sustragerea de informatii personale ale utilizatorului calculatorului) cu care s-a infectat: virus, troian,spyware, etc.

Cum se pot feri utilizatorii de mesajele spam?

Utilizatorii trebuie sa aiba **un produs de securitate complet**, care sa contina si modulul Antispam. In lipsa lui, utilizatorul nu va fi niciodata protejat 100%. Este foarte important detinerea unui program Antipsam.

Exemple de spamming:

- Ajutor pentru un copil bolnav,
- Yahoo/AOL va dona cate 1$ pentru fiecare mail trimis
- Bill Gates face cadou 5000$ si o calatorie la Disney World daca...
- "Retrimite-l la cat mai multi, si de asemenea celui/celei care ti l-a trimis tie ca sa-i arati cat de multi prieteni are"
- Daca nu trimiti acest mesaj in 10 minute la cel putin 7 persoane ti se va intampla ceva ingrozitor. ... etc

Concluzie:

În concluzie, nu deschideți,nu redirecționați mailuri spam și instalați un program Anti-Spam pentru a vă proteja atât calculatorul cât și datele personale.

Keylogger
Ce este keylogger-ul?

Un keylogger este un program care înregistrează fiecare bătaie de tastă pe o tastatură şi salvează aceste date într-un fişier. După ce colectează o anumită cantitate de date, le va transfera prin intermediul internetului unei gazde de la distanţă, predeterminată. De asemenea, poate captura capturi de ecran şi utiliza alte tehnici pentru a urmări activitatea utilizatorului. **Un keylogger poate cauza** pierderea parolelor, date de autentificare, şi alte informaţii similare.

Keylogger: hardware, software

Keyloggerul de tip hardware este un dispozitiv fizic, mic care poate fi lăsat între cablul tastaturii şi portul tastaturii din calculator. Un keylogger de tip hardware poate înregistra toate apăsările de pe tastatură şi le salvează în propria memorie.

Keyloggerii software sunt similari viruşilor şi troianilor. Aceştia sunt utilizaţi de către hackeri pentru a viola intimitatea utilizatorului. Keyloggerii legitimi sunt cunoscuţi şi ca unelte de monitorizare a calculatorului

Activități periculoase ce pot fi inițiate de către keyloggeri:

- Să înregistreze intrările de taste de pe tastatură.
- Să obţină capturi de ecran cu activitatea utilizatorului de pe internet la intervale de timp predeterminate.
- Să urmărească activitatea utilizatorului.
- Să monitorizeze activitatea online a utilizatorului înregistrând adresele website-urilor vizitate, cuvintele cheie introduse şi alte date similare.
- Să înregistreze nume de autentificare, detalii a unor diverse conturi, numerele cardurilor de credit şi parole.
- Să captureze conversaţiile chat-urilor online de pe instant messengers.
- Să obţină copii neautorizate a emailurilor primite şi trimise.
- Să salveze toate datele colectate într-un fişier de pe hard disk, şi să trimită acest fişier unei adrese de email.

Principalele moduri utilizate de către keyloggeri pentru a se infiltra în sistem:

Un keylogger legitim poate fi instalat manual în sistem de către administratorul lui sau de către orice alt utilizator ce are privilegii pentru această activitate. Un hacker poate intra în sistem şi poate seta propriul keylogger.

Keyloggerii maliţioşi pot fi instalaţi în sistem cu ajutorul unui alt parazit precum viruşi, troiani, backdoors şi alte malware-uri.

Cum să eliminați keylogger-ul?

Din nefericire, nu există vreo metodă de recuperare a datelor furate. Din acest motiv, ar trebui să eliminaţi keylogger-ul din calculatorul dumneavoastră cât mai repede posibil. Acest lucru poate fi efectuat utilizând un **anti-spyware reputabil**. Pentru a evita pierderea programelor legitime ce sunt importante pentru funcţionalitatea stabilă a PC-ului, vă recomandăm să utilizaţi unul dintre aceste programe: **Reimage**, **Plumbytes Anti-Malware**.

Spyware
Ce este spyware-ul?

Spyware este o categorie de ameninţări cibernetice, ce descrie programele maliţioase create pentru a infecta sistemele PC-urilor după care să iniţieze activităţi ilegale în acestea. În majoritatea cazurilor, funcţionalitatea acestor ameninţări depinde de intenţiile furnizorilor lor: unele părţi din ameninţările spyware pot fi folosite pentru **a colecta informaţii personale**, în timp ce alţi viruşi de tip spyware îşi pot **urmări victimele** şi colectează informaţii despre obiceiurile lor de navigare.

Pentru ce pot fi utilizate ameninţările de tip spyware:

- Pentru a fura informaţii sensibile.
- Să afişeze reclame nedorite.
- Redirecţionarea utilizatorilor către website-uri chestionabile sau maliţioase contrar dorinţei lor.
- Să creeze numeroase link-uri în rezultatele căutărilor efectuate de victimă şi să îl/o redirecţioneze către locurile dorite.
- Să cauzeze modificări esenţiale în setările sistemului.
- Conectarea la un calculator compromis utilizând backdoors.

Sfaturi pentru eliminarea de spyware:

Pentru a elimina astfel de paraziţi, trebuie să instalaţi unelte speciale anti-spyware (eliminatori de spyware) ce sunt capabile să scaneze sistemul într-un mod similar cu cel al unui software de securitate avansat. Astfel de programe au şi baze de date speciale cu semnăturile paraziţilor ce le permit să detecteze şi să elimine majoritatea ameninţărilor spyware. Aici sunt cei mai puternici eliminatori de spyware: **Reimage**, **Malwarebytes**.

Evită e-mailurile de tip phishing și raportează-le

Un atac de tip **phishing** are loc atunci când cineva încearcă să te păcălească pentru a dezvălui informații personale online.

Ce înseamnă activitatea de phishing?

De obicei, **activitatea de phishing** se face prin **e-mailuri**, anunțuri sau prin intermediul unor site-uri care arată la fel ca site-urile pe care le folosești deja. **E-mailurile sau site-urile de tip phishing** pot să îți ceară:

- nume de utilizator și parole, inclusiv modificări de parolă;
- codul numeric personal;
- numărul contului bancar;
- codurile PIN (numere de identificare personală);
- numărul cardului de credit;
- numele dinainte de căsătorie al mamei tale;
- data nașterii.

Raportează e-mailurile de tip phishing

Când se identifică un **e-mail** care ar putea fi suspect sau de tip **phishing**, e posibil să ți se afișeze un avertisment sau să se mute e-mailul în Spam.

Evită atacurile de tip phishing

Tratează cu atenție **e-mailurile** pe care le primești de la un site care îți solicită informații personale. Dacă primești astfel de e-mailuri:

- nu da clic pe niciun **link** și nu transmite niciun fel de informații personale până când confirmi că e-mailul este real.
- dacă expeditorul are o adresă Gmail, raportează abuzul din Gmail la Google.

Notă: Gmail nu îți va solicita niciodată prin e-mail informații personale precum parola.

Când primești un **e-mail** care pare **suspect**, iată câteva lucruri pe care e recomandat să le verifici:

- verifică dacă adresa de e-mail și numele expeditorului corespund;
- verifică dacă **e-mailul este autentificat**;
- plasează cursorul peste linkuri înainte de a da clic pe ele. Dacă adresa URL a linkului nu corespunde cu descrierea acestuia, e posibil să te direcționeze către un site de tip phishing.
- **verifică antetele mesajelor** pentru a te asigura că antetul „from” nu afișează un nume greșit.