



❖ **Amenințările de tip:**

- **Spam**
- **Spy-ware**
- **Key-loggers**
- **Phishing**

Vladislav Scurtu
Ovidiu Burbulea
clasa a XII-a „T”, IPLT „Mircea Eliade”



Ce este spyware?

- Programe spion.
- Captează ilegal informația de pe calculator precum (parole, nume de indentificare).
- Captează datele de marketing.
- Colectează obiceiurile de navigare pe internet.
- Conduc la mărirea numărului de spam-uri.



Spyware sunt folosite pentru:

- Pentru a fura informații sensibile.
- Să afișeze reclame nedorite.
- Degradarea performanței generale a sistemului și cauzarea instabilității acestuia
- Redirecționarea utilizatorilor către website-uri



Cauza infectării cu spyware:

- ➡ În 99 % din cazuri programul spion este instalat de însuși utilizatorul calculatorului.
- ➡ Se întâmplă la descărcarea diferitor programe ce conțin spyware de pe internet fără a citi licența producătorului.

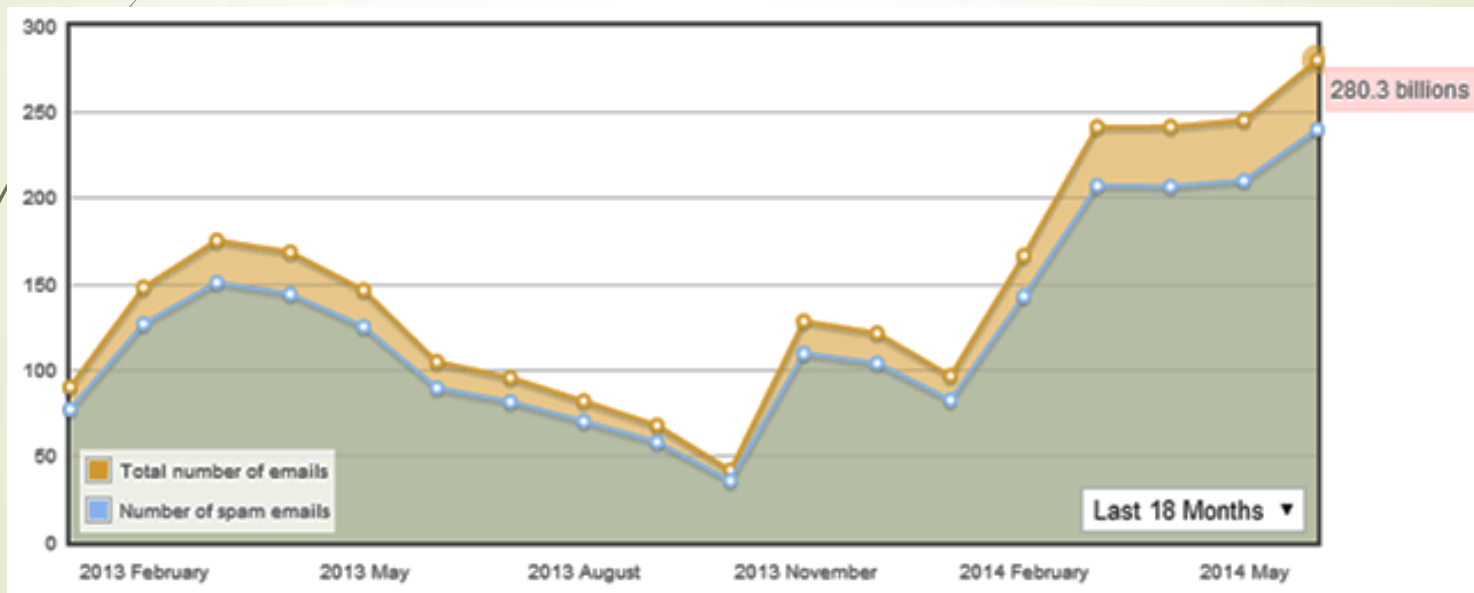


Cum scăpăm de spyware?

- Utilizând unelte speciale anti-spyware.
- Anti-virusii obișnuiți nu îi pot elimina.
- cei mai puternici eliminatori de spyware: Reimage, Malwarebytes.

Ce este un SPAM?

- ➡ Este un mesaj nesolicitat primit pe mail(și nu numai) de obicei în scopuri comerciale.





Cauzele spam-ului :

- Dacă mi-am scris adresa de mail într-un spațiu public.
- Dacă am „adoptat,, un virus pe calculator.
- Persoanele din lista mea de adrese au trimis un e-mail mai departe astfel lăsând adresa mea publică.

Cum ne protejăm de spam-uri ?

- De fiecare dată când trimiteți un email la mai mult de un destinatar si nu este necesar ca aceștia să-și vadă reciproc adresele folosiți, în loc de modul TO (către), modulul BCC (Blind Carbon Copy)
- Nu ne afișăm adresele electronice în nici un loc public de pe internet.
- Ne instalăm un antivirus și scanăm regulat conținutul de pe calculator.

Exemple tipice de spam pe internet

- „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... ,,
- „Daca nu trimiti acest mesaj in 10 minute la cel putin 7 persoane ti se va intampla ceva ingrozitor,,


Ce este phishingul?



Cum să recunoști tentativele de phishing și care sunt riscurile




- Nimeni niciodata nu iti va da bani gratis
- Infractorii mereu lasa mesaje care ii lasa de gol
- Ameninta clientul
- Email-ul contine multe erori gramaticale



Alte sfaturi pentru a te feri de phishing

- Ai grijă la mesajele în care ți se cer informațiile confidențiale
- Nu te lăsa presat
- Fii atent la mesajele generice
- Nu accesa direct link-urile dintr-un mesaj care pare suspect
- Ascultă-ți instinctul



Câteva date îngrijorătoare despre phishing

În 2012-2013, atacurile de tip phishing au afectat, în medie, 102.100 de oameni în fiecare zi la nivel mondial – de două ori mai mulți decât în 2011-2012. Atacurile de phishing au vizat, în principal, utilizatori din Rusia, SUA, India, Vietnam și Marea Britanie.



Ce este un keylogger?

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


Ce poate face un keylogger?

- Să înregistreze intrările de taste de pe tastatură.
- Să obțină capturi de ecran cu activitatea utilizatorului de pe internet la intervale de timp predeterminate.
- Să urmărească activitatea utilizatorului prin înregistrarea titlurilor ferestrelor, numele aplicațiilor lansate, și alte informații specifice.
- Să monitorizeze activitatea online a utilizatorului înregistrând adresele website-urilor vizitate, cuvintele cheie introduse și alte date similare.
- Să înregistreze nume de autentificare, detalii a unor diverse conturi, numerele cardurilor de credit și parole.
- Să captureze conversațiile chat-urilor online de pe instant messengers.
- Să salveze toate datele colectate într-un fișier de pe hard disk, și să trimită acest fișier unei adrese de email.
- Să își complice detectarea și eliminarea.




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 și poate seta propriul keylogger. În ambele cazuri, o amenințare la adresa intimității este instalată în sistem fără știrea sau aprobarea utilizatorului.
- Keyloggerii malițioși pot fi instalați în sistem cu ajutorul unui alt parazit precum viruși, troiani, backdoors și alte malware-uri. Aceștia pot intra în sistem fără știrea utilizatorului și pot afecta pe oricine utilizează un calculator compromis. Astfel de keyloggeri nu au funcții de dezinstalare și pot fi controlați doar de către autorii lor sau atacatori.



Vă mulțumim pentru atenție.
Vă dorim o zi frumoasă în continuare!





Surse:

- <https://ro.wikipedia.org/wiki/Spam>
- <https://www.go4it.ro/internet/despre-spam-si-cum-sa-te-protejezi-de-amenintarile-informaticе-8099663/>
- https://ro.wikipedia.org/wiki/Program_spion
- <http://faravirus.ro/spyware/>
- https://ro.wikipedia.org/wiki/%C3%8En%C8%99el%C4%83ciune_electronic%C4%83
- <https://playtech.ro/2017/ce-inseamna-phishing-si-cum-te-protejezi-de-atacurile-online-malicioase/>
- <http://www.securitatea-informatiilor.ro/tipuri-de-atacuri-informaticе/ce-este-un-keylogger/>
- <http://faravirus.ro/keyloggers/>