

Desmitificant els virus informàtics

Associació Hacking Lliure

24 d'octubre de 2018



Índex

- 1 Presentació**
- 2 Què és un virus informàtic?**
- 3 Què és la enginyeria social?**
- 4 Què és una vulnerabilitat de software?**
- 5 Conclusió**

Índex

- 1 Presentació**
- 2 Què és un virus informàtic?**
- 3 Què és la enginyeria social?**
- 4 Què és una vulnerabilitat de software?**
- 5 Conclusió**

About

Hacking Lliure

- Associació de Hacking Ètic i Seguretat Informàtica
- Gestada a les acaballes del 2016 per estudiants de la facultat
- Constituïda formalment a principis del 2017
- UB & Catalunya
- Presentació oficial: 27/02/17

Índex

- 1 Presentació**
- 2 Què és un virus informàtic?**
- 3 Què és la enginyeria social?**
- 4 Què és una vulnerabilitat de software?**
- 5 Conclusió**

Definició col·loquial

Un **virus informàtic** és un programa que “infecta” o “ataca” un ordinador.

Definició col·loquial

Un **virus informàtic** és un programa que “infecta” o “ataca” un ordinador.

Un **virus informàtic** és un segment de línia de codi que altera el funcionament normal de l’ordinador, sense el permís o el coneixement de l’usuari.

Definició formal: Malware

Un **virus informàtic** és un programa que “infecta” o “ataca” un ordinador.

Definició formal: Malware

Un **virus informàtic** és un programa que “infecta” o “ataca” un ordinador.

El **malware** (o programari maliciós) és qualsevol programa informàtic intencionalment dissenyat per a actuar en contra dels interessos de l’usuari.

Virus

Un **virus informàtic** és un tipus de malware el qual, un cop executat, és replica modificant altres programes i insertant el seu propi codi.

Tipus (no exclusius) de malware

- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors

Tipus (no exclusius) de malware

- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors

Tipus (no exclusius) de malware

- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors

Tipus (no exclusius) de malware

- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors



Tipus (no exclusius) de malware

- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors

Tipus (no exclusius) de malware

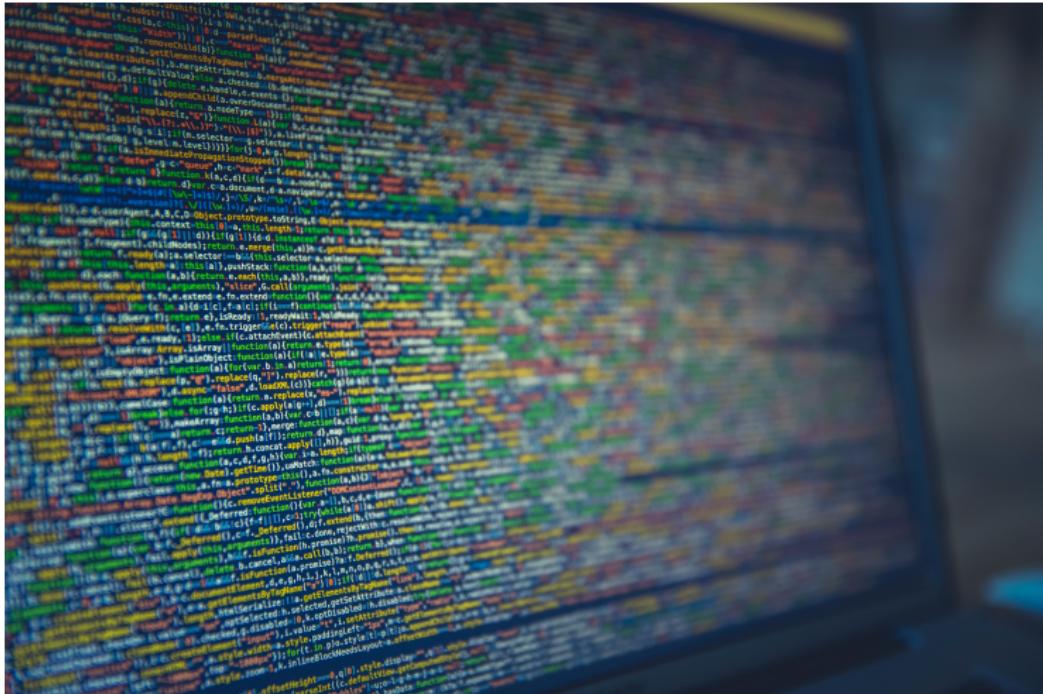
- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors

Tipus (no exclusius) de malware

- Virus
- Spyware
- Adware
- Ransomware
- Remote Access Trojan (RAT)
- Rootkit/Bootkits
- Backdoors

***The Intel ME
is still on,
even when your
computer is off.***

Com aconsegueix el malware actuar contra l'usuari?



Com aconsegueix el malware actuar contra l'usuari?

- Enginyeria social
- Vulnerabilitats

Índex

- 1 Presentació**
- 2 Què és un virus informàtic?**
- 3 Què és la enginyeria social?**
- 4 Què és una vulnerabilitat de software?**
- 5 Conclusió**

Enginyeria social

La **enginyeria social**, en el camp de la seguretat de la informació, es refereix a la manipulació psicològica de persones per a provocar que facin accions o divulguin informació confidencial.

Enginyeria social

Utilitza tècniques de manipulació com:

- Reciprocitat
- Compromís i consistència
- Influència social
- Autoritat

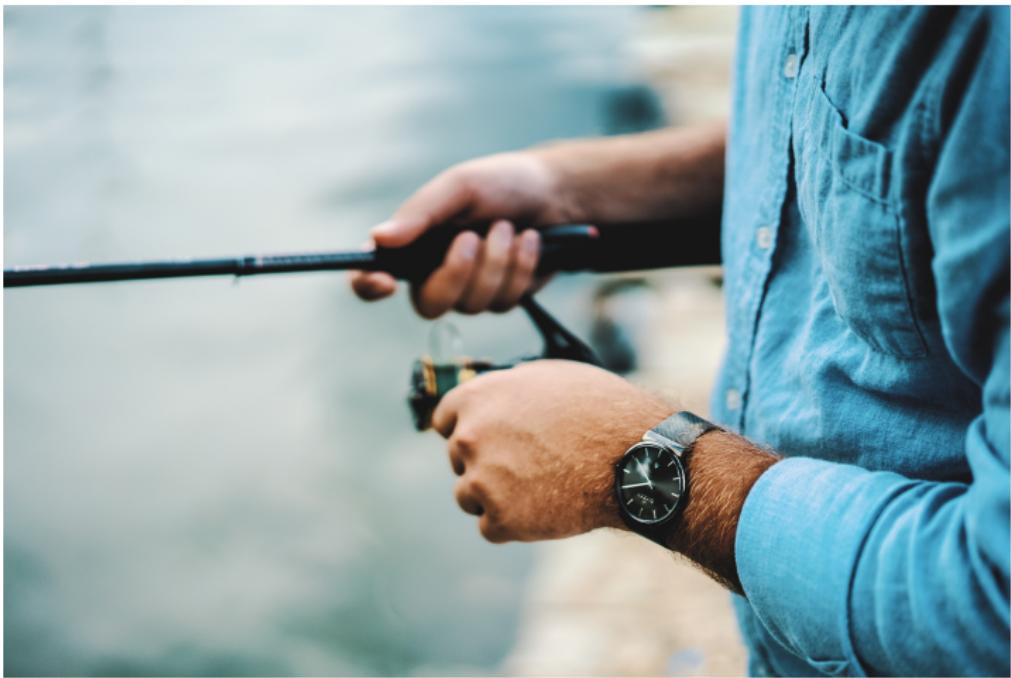
Phishing

Els objectius són contactats per correu electrònic, telèfon o missatge de text per algú presentant-se com a institució lègítima, i pressionats per a proporcionar dades sensibles.

Tailgating

Un atacant, buscant entrada a una àrea restringida, senzillament entra mitjançant una persona que té accés legítim, utilitzant alguna tècnica de manipulació.

Baiting



Baiting

Distribuir USBs al pàrquing d'una organització que es vol atacar, que continguin un malware que infecti els ordinadors on siguin connectats.

Només cal esperar que algun dels empleats n'agafi un i el connecti al seu ordinador per aconseguir accés a l'organització.

Índex

- 1 Presentació**
- 2 Què és un virus informàtic?**
- 3 Què és la enginyeria social?**
- 4 Què és una vulnerabilitat de software?**
- 5 Conclusió**

Vulnerabilitat

Una **vulnerabilitat** és una feblesa d'un sistema que permet a un atacant violar la integritat, la privadesa, el control d'accés, la disponibilitat, les dades o els programes d'aquest.

Buffer overflows

```
char *mail_auth(char *mechanism, authresponse_t resp, int argc, char *argv[])
{
    char tmp[MAILTMPLEN];
    AUTHENTICATOR *auth;
    /* make upper case copy of mechanism name */
    ucase(strncpy(tmp, mechanism));
    for(auth = mailauthenticators; auth; auth = auth->next)
        if(auth->server && !strcmp(auth->name, tmp))
            return (*auth->server)(resp, argc, argv);
    return NIL;      /* no authenticator found */
}
```

Figura: University of Washington's IMAP server, corrected in 1998

Integer overflows

```
#include <stdio.h>

void main() {
    unsigned int num1 = 4294967295;
    int num2 = 4294967295;
    unsigned int num3 = 4294967297;
    int num4 = 4294967297; █

    printf("%ld\n", num1);
    printf("%d\n", num2);
    printf("%ld\n", num3);
    printf("%d\n", num4);
}
```

Integer overflows

```
#include <stdio.h>

void main() {
    unsigned int num1 = 4294967295;
    int num2 = 4294967295;
    unsigned int num3 = 4294967297;
    int num4 = 4294967297;

    printf("%ld\n", num1);
    printf("%d\n", num2);
    printf("%ld\n", num3);
    printf("%d\n", num4);
}
```

```
[dabytmc@LibrePad demos]$ ./a.out
4294967295
-1
1
1
```

Integer overflows

```
nresp = packet_get_int();
if(nresp > 0)
{
    response = xmalloc(nresp * sizeof(char *));
    for(i = 0; i < nresp; i++)
        response[i] = packet_get_string(NULL);
}
```

Figura: OpenSSH in versions prior to 3.4

Índex

- 1 Presentació**
- 2 Què és un virus informàtic?**
- 3 Què és la enginyeria social?**
- 4 Què és una vulnerabilitat de software?**
- 5 Conclusió**

Conclusió

Conceptes

- El que entenem col·loquialment com un virus és en realitat malware.
- Els virus són un tipus de malware.
- La seguretat absoluta no existeix.
- El malware no és màgia: funciona gràcies als errors humans i les vulnerabilitats.

Conclusió

Conceptes

- El que entenem col·loquialment com un virus és en realitat malware.
- Els virus són un tipus de malware.
- La seguretat absoluta no existeix.
- El malware no és màgia: funciona gràcies als errors humans i les vulnerabilitats.

Conclusió

Conceptes

- El que entenem col·loquialment com un virus és en realitat malware.
- Els virus són un tipus de malware.
- La seguretat absoluta no existeix.
- El malware no és màgia: funciona gràcies als errors humans i les vulnerabilitats.

Conclusió

Conceptes

- El que entenem col·loquialment com un virus és en realitat malware.
- Els virus són un tipus de malware.
- La seguretat absoluta no existeix.
- El malware no és màgia: funciona gràcies als errors humans i les vulnerabilitats.

Conclusió

Consells

- Per a evitar ser enganyats o utilitzats, hem de desconfiar i actuar sempre valorant correctament les situacions.
- Per a reduir les vulnerabilitats dels nostres ordinadors, cal escollir correctament i actualitzar els programes que instal·lem.
- Per a més seguretat, existeixen eines com els antivirus, encara que aquests realitzen una tasca reactiva contra mostres conegudes, però no protegeixen contra atacs nous o dirigits.
- Si desenvoleueu algún programa que voleu distribuir, teniu sempre en compte la seguretat.

Conclusió

Consells

- Per a evitar ser enganyats o utilitzats, hem de desconfiar i actuar sempre valorant correctament les situacions.
- Per a reduir les vulnerabilitats dels nostres ordinadors, cal escollir correctament i actualitzar els programes que instal·lem.
- Per a més seguretat, existeixen eines com els antivirus, encara que aquests realitzen una tasca reactiva contra mostres conegudes, però no protegeixen contra atacs nous o dirigits.
- Si desenvoleueu algún programa que voleu distribuir, teniu sempre en compte la seguretat.

Conclusió

Consells

- Per a evitar ser enganyats o utilitzats, hem de desconfiar i actuar sempre valorant correctament les situacions.
- Per a reduir les vulnerabilitats dels nostres ordinadors, cal escollir correctament i actualitzar els programes que instal·lem.
- Per a més seguretat, existeixen eines com els antivirus, encara que aquests realitzen una tasca reactiva contra mostres conegudes, però no protegeixen contra atacs nous o dirigits.
- Si desenvoleueu algún programa que voleu distribuir, teniu sempre en compte la seguretat.

Conclusió

Consells

- Per a evitar ser enganyats o utilitzats, hem de desconfiar i actuar sempre valorant correctament les situacions.
- Per a reduir les vulnerabilitats dels nostres ordinadors, cal escollir correctament i actualitzar els programes que instal·lem.
- Per a més seguretat, existeixen eines com els antivirus, encara que aquests realitzen una tasca reactiva contra mostres conegudes, però no protegeixen contra atacs nous o dirigits.
- Si desenvolupueu algún programa que voleu distribuir, teniu sempre en compte la seguretat.

Gràcies per la vostra atenció



<https://hackinglliure.org>

<https://twitter.com/hackinglliure>

info@hackinglliure.com