#AprenemCiberseguretat

MALWARE

Què és?

PROGRAMA INFORMÀTIC QUE PRINCIPALMENT S'EXECUTA SENSE EL CONEIXEMENT NI AUTORITZACIÓ DEL PROPIETARI O PROPIETÀRIA DE L'EQUIP INFECTAT. ELS SEUS OBJECTIUS SÓN EL ROBATORI D'INFORMACIÓ, EL SEGREST DE L'EQUIP O DADES DEL SISTEMA I/O RECLUTAMENT PER A UNA XARXA DE *BOTS*.

Tipus de *malware*

RANSOMWARE
El seu objectiu és "segrestar" un dispositiu o la informació que conté, de manera que, si la víctima no paga el rescat, no podrà accedir-hi.

SPYWARE
Recopila informació del comportament de l'usuari/ària durant la seua navegació. Després l'envia a una entitat remota sense el coneixement o consentiment del propietari/ària de l'ordinador.

KEYLOGGER
Monitora tota l'activitat realitzada amb el teclat (tecles que es premen) per a després enviar-la al ciberdelinqüent.

BOTS
Infecta l'ordinador i l'inclou en una xarxa d'ordinadors controlats per un servidor central gestionat pel ciberdelinqüent per a finalitats com utilitzar l'equip per a atacar altres servidors.

MALVERTISING
Anunci, bàner publicitari o finestra emergent que apareix visitant una web. Redirigeix o carrega contingut d'un altre lloc web on s'allotja el *malware* que es descarregarà en l'ordinador.

VIRUS
S'instal·la dins del codi d'un programa de l'equip objectiu, i, quan aquest s'executa, infecta altres fitxers del sistema.

BACKDOORS
Crea portes posteriors utilitzades pels atacants per a continuar controlant l'ordinador compromés i passant inadvertides per a l'usuari/ària.

ROOTKITS
Oculta la presència del *software* maliciós en l'ordinador, evitant que el programari de detecció (antivirus, *logs* del sistema, comandos d'administració) revele la seua presència.

CUC
Es replica i es mou per les xarxes d'ordinadors de manera autònoma, buscant noves víctimes per a infectar. Els cucs no requereixen interacció amb l'usuari/ària per a propagar-se.

TROIÀ
Es fa passar per un *software* inofensiu, però inclou una part maliciosa oculta, que permet a l'atacant interactuar amb l'ordinador de la víctima sense que aquesta se n'adone.

BONES PRÀCTIQUES

1. Utilitzeu **CONTRASENYES ADAPTADES A LA FUNCIONALITAT**. Si és possible, useu doble autenticació.
2. **NO OBRIU CAP ENLLAÇ** ni descarregueu cap fitxer adjunt procedent d'un correu o missatge que presente qualsevol indici o patró fora de l'habitual.
3. Useu **PROGRAMARI DE SEGURETAT**, eines antivirus i *antimalware*, tallafocs personals, eines d'esborrament segur, etc.
4. Manteniu **ACTUALITZADES LES APLICACIONS I EL SISTEMA OPERATIU** per a evitar donar facilitats a la potencial amenaça.
5. **NO INSTAL·LEU PROGRAMES** des de llocs no oficials.
6. **ESBORRAMENT SEGUR** de la informació una vegada ja no és necessària.
7. Realitzeu **CÒPIES DE SEGURETAT** periòdiques. En cas d'infecció amb codi nociu, pèrdua de dades, avaries del *hardware* d'emmagatzematge, esborrament d'informació involuntària per part de l'usuari o usuària, es podrà recuperar la informació.
8. Reviseu regularment la **CONFIGURACIÓ DE SEGURETAT** aplicada, els permisos de les aplicacions i les opcions de seguretat.
9. **ENCRIPTEU LA INFORMACIÓ SENSIBLE.**
10. Limiteu la **SUPERFÍCIE D'EXPOSICIÓ DE LES AMENACES**. Determineu serveis estrictament necessaris.

WWW.UV.ES/UVSTIC

VNIVERSITAT DE VALÈNCIA UVstic

Vicerectorat d'Estratègia, Qualitat i Tecnologies de la informació
Conscienciació en la seguretat de la informació