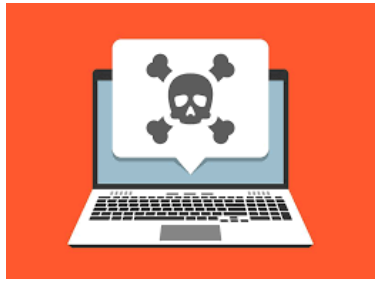
Agència Nacional de Ciberseguretat d'Andorra

Conscienciació en ciberseguretat

Prevenció d'infeccions per Malware i protecció contra el Ransomware



Malware és un terme genèric que s'utilitza per qualsevol **tipus de programari maliciós** que ha estat dissenyat amb l'objectiu de causar **danys** o **aprofitar vulnerabilitats de qualsevol xarxa, servei o dispositiu que pugui ser programable.**

Els ciberdelinqüents el solen fer servir per **extreure dades** que poden aprofitar per prendre **diners a les víctimes.**

Aquestes dades poden ser des **d'informació financera** fins a **registres mèdics, missatges personals al seu correu electrònic** o les seves **contrasenyes personals** o **professionals.**

Els tipus d'informació que poden córrer perill, avui dia, són **innombrables** i de diferent índole.

Les dades que obtenen els ciberdelinqüents són, sobretot, informació de caràcter financera, missatges personals del correu electrònic de les víctimes o, fins i tot, les seves contrasenyes personals o professionals.

Per què als ciberdelinqüents els agrada fer servir el *malware* per cometre els seus ciberdelictes?

El ***malware*** abasta tota mena de **programaris maliciosos**, inclosos els virus i els ciberdelinqüents el fan servir per a molts **FINS** diferents.

1. Enganyar la víctima perquè els facilitin les seves dades personals i així poder robar la seva identitat personal

2. Infectar els ordinadors de les seves víctimes i usar-los per extreure bitcoins o altres criptodivises

3. Robar dades de la targeta de crèdit d'una web dels seus clients o altres dades financeres/econòmiques

4. Assumir el control de diversos ordinadors per tal de llançar atacs de Denegació de Servei contra altres xarxes

Tipus de *malware*

En l'actualitat, existeix un gran ventall de programari maliciós i cada dia van creant-se i apareixent més tipus diferents. Seria convenient que coneguem les seves **TIPOLOGIES**, per tal de protegir millor les nostres dades i dispositius.

1. Virus

Els virus solen transmetre's a través **d'arxius adjunts de missatges de correu electrònic** que contenen la càrrega viral o l'arxiu executable del *malware* que duu a terme la infiltració maliciosa. Quan la víctima obre l'arxiu, el dispositiu s'infecta.

2. Ransomware

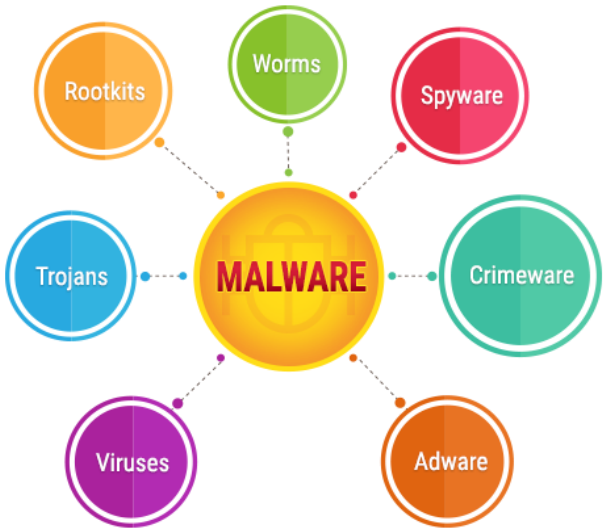
Aquest tipus de *malware* és un dels **tipus més rendibles i més populars** entre els ciberdelinqüents. Aquest s'instal·la al dispositiu de la víctima, xifra els seus arxius i, a continuació, li exigeix un **rescat**.

3. Scareware

Els ciberdelinqüents **atemoreixen les víctimes** fent-les pensar que els seus ordinadors o *smartphones* s'han infectat i les **convencen perquè comprin una aplicació falsa**.

4. Cucs

Els cucs tenen la capacitat de replicar-se d'un dispositiu a un altre, aprofitant algun tipus de **punt feble de seguretat en un programa o sistema operatiu** i no requereixen la interacció de l'usuari per funcionar.



Tipus de *malware*

En l'actualitat, existeix un gran ventall de programari maliciós i cada dia van creant-se i apareixent més tipus diferents. Seria convenient que coneguem les seves **TIPOLOGIES**, per tal de protegir millor les nostres dades i dispositius.

5. Spyware

Es tracta d'un **programa que s'instal·la al teu ordinador i sense el teu coneixement explícit per tal de capturar i transmetre informació personal o hàbits de navegació a Internet** i altres dades al seu usuari.

6. Troians

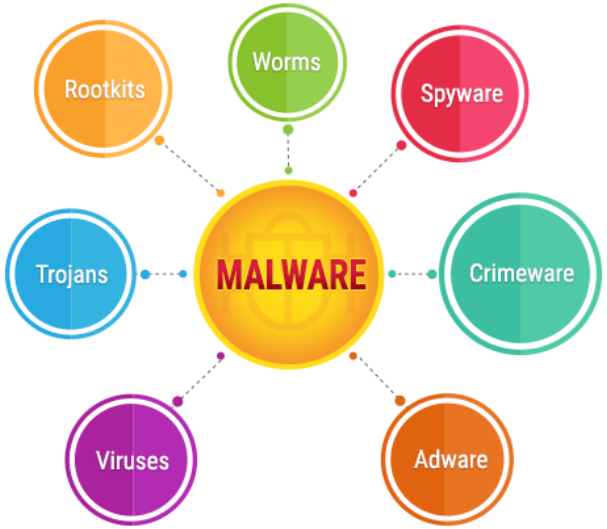
Els troians es disfressen d'**aplicacions inofensives amb l'objectiu d'enganyar els usuaris perquè les descarreguin i les usin**. Un cop en funcionament, poden **robar dades personals, bloquejar-te el teu dispositiu, espiar activitats** o fins i tot **llançar un atac**.

7. Adware

Els programes d'*adware* envien **anuncis no desitjats als usuaris i solen mostrar cartells parpellejant o finestres emergents** al mateix temps que l'usuari realitza una determinada acció.

6. Malware sense arxius

El *malware* sense arxius és un tipus de programari maliciós que utilitza **programes autèntics per infectar un equip**. Aquest llança un **atac de registre**, no deixa arxius de *malware* que es puguin analitzar ni tampoc processos maliciosos que puguin ser detectats.



Com es propaga un *malware*?

El *malware* es fa servir per atacar a través de: arxius adjunts de correu electrònic, anuncis maliciosos en llocs web, instal·lacions de Programari fraudulent, unitats USB i aplicacions infectades, correus electrònics de *phishing* i missatges de text.

Com sé si m'han infectat amb un Malware?

- ✓ Rendiment lent del seu equip.
- ✓ Redireccions del navegador, és a dir, quan el seu navegador el porta a llocs web que no tenia intenció de visitar.
- ✓ Advertències d'infecció acompanyades d'ofertes per comprar alguna cosa i així solucionar el problema.
- ✓ Problemes per encendre o apagar l'equip.
- ✓ Anuncis emergents freqüents.

CONCLUSIÓ: Com més d'aquests símptomes habituals vegis, més gran serà la probabilitat que el seu ordinador estigui infectat amb un Malware.

Com podeu protegir-vos del *malware*?

Tot i que hi ha molts tipus de *malware*, la part positiva és que també hi ha moltes formes de què us pugueu protegir d'aquests. Presteu atenció a aquests **CONSELLS** que us donem en aquesta diapositiva i incloeu-la en la vostra vida diària.

Protegiu bé els vostres dispositius personals

- ✓ És molt important que mantingueu tot el temps **actualitzat el teu sistema operatiu i les teves aplicacions.** Els ciberdelinqüents busquen les vulnerabilitats en Programaris que són antics o estan obsolets.
- ✓ Mai feu **clic en un vincle** que vegeu en una **finestra emergent.**
- ✓ **Limiteu la quantitat d'aplicacions que teniu instal·lades als vostres dispositius.** Tingueu només les aplicacions que cregueu que necessiteu realment i que utilitzeu en el vostre dia a dia.
- ✓ Utilitzeu una **solució de seguretat mòbil**, ja que les campanyes de ***malware*** **i** ***adware*** continuen infectant aplicacions mòbils.
- ✓ **No presteu el vostre telèfon ni deixeu els vostres dispositius desatesos per cap motiu.** Si la vostra configuració predeterminada ha canviat o una nova aplicació ha aparegut de manera misteriosa pot ser un senyal que un programa de ***spyware*** se us hagi instal·lat sol.

Presteu atenció a les descàrregues i a les compres de programari que realitzeu

- ✓ **Compreu només programari de seguretat a empreses de confiança** i sempre a través del seu lloc o botiga oficial.
- ✓ **Assegureu-vos bé de descarregar només allò que us inspiri confiança**. És bo que llegiu les ressenyes de les aplicacions que us voleu descarregar i utilitzeu només les botigues d'aplicacions oficials.
- ✓ **No obriu les dades adjuntes que venen annexades a missatges de correu electrònic** quan no sapigueu que venen d'una font fiable.

Com podeu protegir-vos del *malware*?

Tot i que hi ha molts tipus de *malware*, la part positiva és que també hi ha moltes formes de què us pugueu protegir d'aquest. Presteu atenció a aquests **CONSELLS** que us donem en aquesta diapositiva i incloeu-la en la vostra vida diària...

Tingueu molta cura amb la vostra activitat i la vostra navegació per Internet

- ✓ **Hauríeu d'evitar fer clic a vincles desconeguts**. Dona igual si el rebeu a través d'un correu electrònic, una xarxa social o un missatge de text. **Si un vincle no us resulta familiar, eviteu obrir-lo.**
- ✓ Sigueu més selectiu sobre els llocs web que visiteu. És bo utilitzar un **complement de recerca segur** i evitar qualsevol lloc web que pugui ser maliciós.
- ✓ **Tingueu molta cura amb els correus electrònics en els quals us demanen informació personal.** Si rebeu un correu electrònic en el qual apareix, per exemple, el vostre banc i aquest us està indicant que hauríeu d'accedir a un vincle i restablir la vostra contrasenya o accedir a l'àrea personal del vostre banc, per favor, **no hi feu clic.**
- ✓ **Eviteu sempre els llocs web de risc** com per exemple, els que us ofereixen fons de pantalla totalment gratuïts.

Dueu a terme controls cada cert temps

Si us preocupa que el vostre dispositiu pugui estar infectat, **seria bo que executéssiu una anàlisi utilitzant el Programari de seguretat** que tinguéssiu instal·lat.

- ✓ Reviseu cada X temps els vostres **comptes bancaris i els informes de crèdit.**

Com reaccionar en cas de tenir problemes amb aquesta pràctica?

El **Ransomware** és una **extorsió** que es realitza a través d'un **malware** que s'introdueix als equips de les empreses (ordinadors, portàtils i dispositius mòbils).

Aquest programari maliciós **segresta la informació de l'empresa**, impedint l'accés a la mateixa i demanant per això un **RESCAT** a canvi de l'alliberament de les dades segrestades. A les empreses, això està causant nombroses **pèrdues temporals o permanents d'informació i interrompent l'activitat normal** de l'empresa i ocasionant **pèrdues econòmiques i importants danys en la REPUTACIÓ de l'usuari afectat.**

Aquest tipus d'atac està creixent de forma considerable, ja que és molt rendible per als delinqüents realitzar aquest tipus d'accions:

- ✓ Cada vegada hi ha més **dispositius que són potencialment senzills de segrestar.**
- ✓ És més senzill segrestar la informació a causa dels avenços que hi ha en matèria de **Criptografia.**
- ✓ Els ciberdelinqüents poden **ocultar la seva activitat** per llançar atacs massius.
- ✓ En emprar **sistemes de pagament anònim d'índole internacional** és més difícil el seguiment del delicte.

Teniu un Ransomware a la vostra empresa o organització?

Si la vostra empresa o organització s'ha vist afectada per un Ransomware, el més **IMPORTANT** que heu de fer és **NO PAGAR MAI EL RESCAT.**

I per què no podeu pagar el rescat?

- ✓ Pagar no us garantirà que torneu a tenir accés a les dades que us han estat segrestades. **Recordeu que esteu tractant amb delinqüents.**
- ✓ Si pagueu és possible que sigueu objectiu d'**atacs posteriors** donat que, **el segrestador ja sap que esteu disposats a pagar**.
- ✓ Pot ser que us demanin una **xifra major** un cop els hàgiu pagat.
- ✓ Pagar **fomenta i ajuda a mantenir el negoci** d'aquests tipus de ciberdelinqüents.