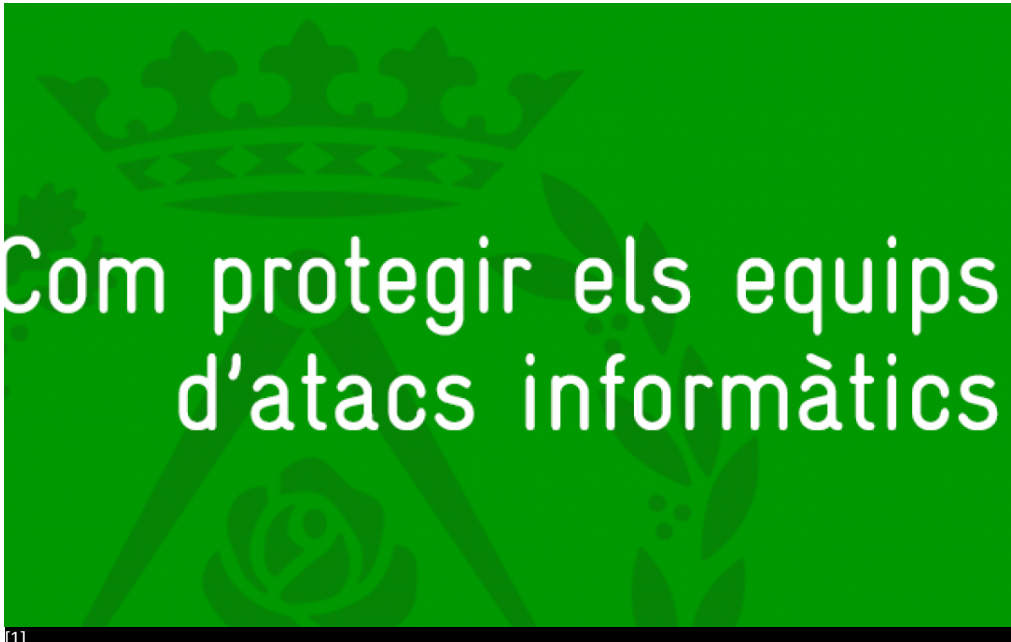




Com protegir els equips d'atacs informàtics

[1]

Com protegir els teus dispositius dels atacs informàtics

Imatge:

© Col·legi d'Arquitectes de Catalunya (COAC)

La setmana passada va haver-hi un atac massiu mitjançant codi maliciós de tipus *ransomware*, que ha afectat un gran nombre d'organitzacions a nivell estatal. Tot i que el COAC no ha estat afectat, informem als col·legiats de les problemàtiques que l'atac pot ocasionar.

El *ransomware*, de la variant WannaCry, pot infectar els equips informàtics que utilitzen el sistema operatiu **Windows**. Una vegada infectat un ordinador, el virus es distribueix a la resta de màquines Windows que hi hagi en la mateixa xarxa.

Les formes per les quals un ordinador es pot infectar són les següents:

- *Phishing* mitjançant correu electrònic que contingui un enllaç a un web o un fitxer adjunt.
- Accedint a pàgines web infectades amb un navegador sense actualitzar o que tingui plugins desactualitzats o no segurs.

Els sistemes afectats (dels quals ja hi ha una actualització de seguretat disponible a

Microsoft), són:

- Windows Vista SP2
- Windows Server 2008 SP2 i R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 i R2
- Windows 10
- Windows Server 2016

Consells i recomanacions:

El Centre de Seguretat de la Informació de Catalunya (CESICAT) ha publicat els següents consells i recomanacions:

- Actualitzar el sistema operatiu Windows a la seva última actualització per a una protecció adient davant aquesta ciberamença.
- Assegurar-vos que els arxius adjunts són documents que estàveu esperant. En el cas que no estigueu esperant aquests fitxers, es recomana eliminar el correu rebut i no obrir-lo per precaució a infectar l'ordinador.
- Mantenir la versió d'antivirus actualitzada a la darrera versió, així com els complements de seguretat i tallafocs.
- Realitzar còpies de seguretat dels arxius amb regularitat, almenys els més importants. Un atac *ransomware* no suposa un problema sempre que es mantingui una còpia de seguretat dels seus arxius.
- Utilitzar un servei antimalware eficaç. Hi ha eines de seguretat que identifiquen el comportament específic d'un *ransomware* i bloquegen la infecció abans que pugui causar danys.
- En cas de resultar afectat per un atac de tipus *ransomware* es recomana apagar l'ordinador i desconnectar-lo de la xarxa. Posteriorment, posar-se en contacte amb un tècnic informàtic.

En **aquesta pàgina web** ^[2] trobareu més informació i una explicació més detallada sobre aquest virus.

Bones pràctiques:

Recordem, en general, observar les següents bones pràctiques en matèria de seguretat, per evitar la introducció d'elements maliciosos al vostre ordinador i, per extensió, a tota l'organització:

- No obrir pàgines webs amb dubtosa o mala reputació.
- Prestar especial atenció i mostrar-se previnguts enfront de missatges de correu que:
- Sol·licitin informació personal o dades d'accés (el COAC mai demanarà un usuari o contrasenya via correu electrònic).

- Continguin arxius o adjunts que no esperem o amb noms o formats no familiars.
- Provinguin d'adreces de correu electrònic desconegudes, però alhora "familiars" (p. ex. administrador.coac@hotmail.com [3], coac@gmail.com [4]).
- Que el text exigeixi urgència, contingui amenaces o busqui generar alarma.
- El text del missatge contingui idiomes desconeguts, un estil poc familiar o tingui paraules, expressions o concordances de gènere mal escrites.
- Semblin missatges massa bons per ser veritat (com a premis, viatges gratis, etc).

13/05/2017

Tornar [5]

Copyright@ Col·legi d'Arquitectes de Catalunya : <http://coac.arquitectes.cat/ca/suport/actualitat/atac-massiu-de-ransomware>

Links:

- [1] <http://coac.arquitectes.cat/ca/suport/actualitat/atac-massiu-de-ransomware>
- [2] <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-16-ransomware-1/file.html>
- [3] <mailto:administrador.coac@hotmail.com>
- [4] <mailto:coac@gmail.com>
- [5] <http://coac.arquitectes.cat/ca/javascript%3Ahistory.back%281%29>