Aviso importante sobre "ciberataque" de ransomware

¿De qué se trata?

Desde el pasado viernes 12 de mayo un malware (virus) se está difundiendo a nivel mundial. Esto es algo que, por desgracia, ocurre a diario, pero en esta ocasión, por diferentes motivos, ha tenido mayor repercusión de la habitual en los medios de comunicación.

Una vez que este malware entra en la red de una organización, se puede transmitir entre sus ordenadores con sistema Windows a través de una vulnerabilidad para la que existe una solución (una actualización del sistema).

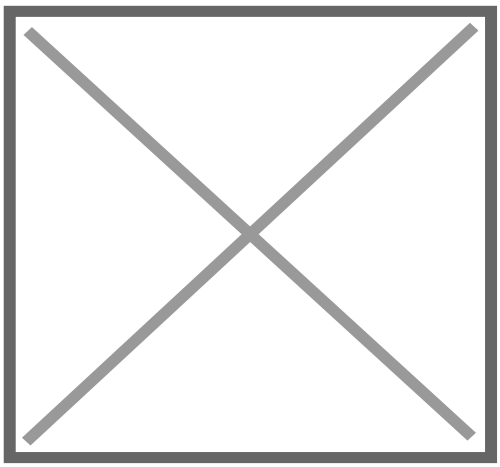
Si un equipo se infecta, se cifrarán y quedarán inutilizables tanto **sus ficheros** como los de los dispositivos (pendrives, disco duros externos, carpetas de red compartidas, Google Drive, Dropbox…) a los que tenga acceso. Actualmente no se conoce una forma de recuperar esta información salvo a partir de una copia de seguridad.

¿Qué debo hacer para prevenir?

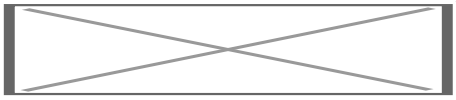
Este problema sólo afecta a equipos con sistema operativo Windows. Si es su caso, siga estas indicaciones:

1. No abra ningún correo de remitentes desconocidos con ficheros adjuntos sospechosos.
2. Sea especialmente cuidadoso con la navegación web. Navegue solo por sitios web fiables y necesarios para el desempeño de su trabajo.
3. Compruebe que su sistema está actualizado. Si su equipo se lo ha entregado e instalado el Servicio de Informática, ya estará configurado de forma que las actualizaciones importantes del sistema se descargan de forma automática cuando Microsoft las publica y, por tanto, no estaría en riesgo. No obstante, realice esta comprobación, ya que, es posible que dado que Vd. es administrador de su sistema, en algún momento haya modificado esta configuración o bien, no haya querido o podido instalar estas actualizaciones.

   En Windows: Teclee “Windows Update” en el control de búsqueda y, después, pulse sobre “Buscar actualizaciones”

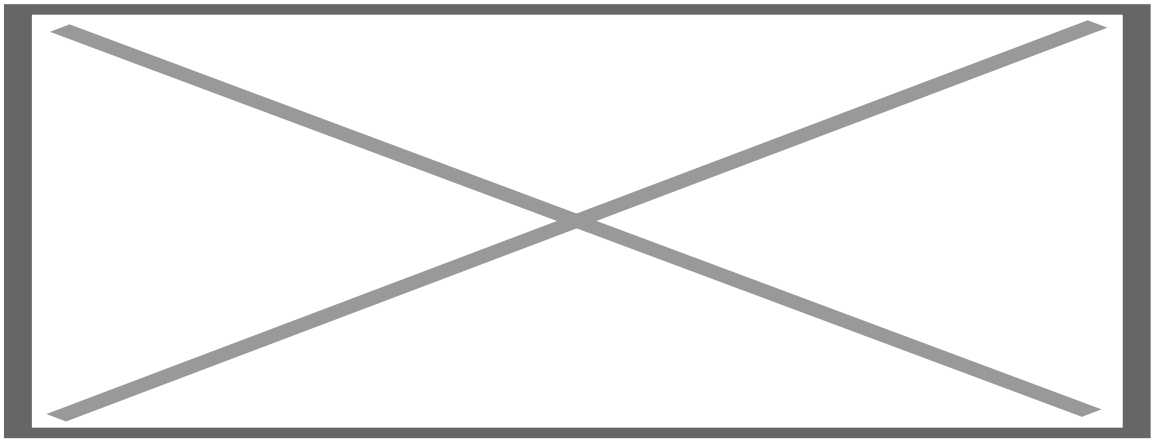


Si tiene todas las actualizaciones importantes instaladas verá lo siguiente:



Si no fuera así, pulse sobre “buscar las actualizaciones” importantes disponibles e instálelas.

4. Compruebe que tiene activada la instalación automática de actualizaciones importantes:



5. Compruebe que tiene su antivirus actualizado. Recuerde que puede instalar la última versión del antivirus Panda de la UJA desde: http://www.uja.es/conocenos/servicios-unidades/sinformatica/software/antivirus/particular
6. Recuerde que si su equipo se infecta y sus ficheros son cifrados, la única solución posible actualmente de recuperar su información es a partir de una copia de seguridad. En cuanto pueda, realice una copia de seguridad de su información en un dispositivo externo y desconéctelo de su equipo una vez realizada la copia. Puede seguir estas recomendaciones del Servicio de Informática: http://www.uja.es/conocenos/servicios-unidades/sau/guias/microinformatica/copia_seguridad

Seguiremos informando en esta misma página web

Más información

- CCN-CERT: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- Microsoft: https://blogs.technet.microsoft.com/microsoftlatam/2017/05/13/orientacion-al-cliente-para-ataques-wannacrypt/