1.-Qué es el ransomware

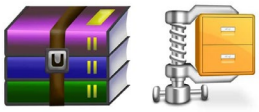
Podemos definir el ransomware como un tipo de malware (software malicioso) que bloquea el uso de un dispositivo (ordenador, tablet, smartphone…) o la información que contiene, para después pedir un rescate a cambio de su recuperación.

Ransomware

El método más habitual de propagación es a través del envío de correos electrónicos maliciosos a las víctimas.

Correo

Los engañan para que abran un archivo adjunto infectado (zip o rar) o hagan clic en un enlace que les lleva al sitio web del atacante, dónde se infectan. Una vez infectados, mediante un mensaje, que suele ser intimidante, avisan a la víctima de que la única forma en que puede descifrar sus archivos o recuperar el sistema es pagar al cibercriminal.



Archivos en extensión .rar o .zip

2.-Cómo nos podemos infectar

Las vías más habituales de infección por *ransomware* suelen ser las siguientes:

-Aprovechar **agujeros de seguridad (vulnerabilidades) del software.**

Actualizaciones del sistema.

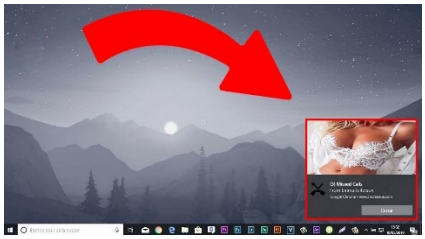
-Engañar a los usuarios, mediante **técnicas de ingeniería social**, **para que instalen el malware.**

Solicitud de Informacion.

-Mediante **SPAM (correo basura)** que contiene enlaces web maliciosos o ficheros adjuntos que descargan el malware.

Correo con publidad.

-También utilizan técnicas de ***malwertising*** (incrustan anuncios maliciosos en sitios web legítimos).



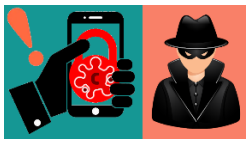
Paginas indecorosas o de dudosa Procedencia.

-***Drive-by-download,*** consiste en dirigir a las víctimas a sitios web infectados, descargando el malware sin que ellas sean conscientes, aprovechando las vulnerabilidades de su navegador.

Paginas con extensiones irreales www.facebook.com.sus

3.- Prevenir la infección por ransomware

-Es una técnica psicológica que consiste en engañar a los usuarios suplantando la identidad de personas importantes o conocidas de la organización, intentando que las víctimas les den acceso para instalar el malware.



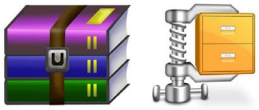
-Desconfía de cualquier mensaje recibido por correo electrónico, SMS, Whatsapp o redes Sociales.

-No abras correos de usuarios desconocidos o que no hayas solicitado: elimínalos directamente, no contestes nunca a estos correos.

-Revisa los enlaces antes hacer clic, aunque sean de contactos conocidos. Desconfía de los enlaces acortados.

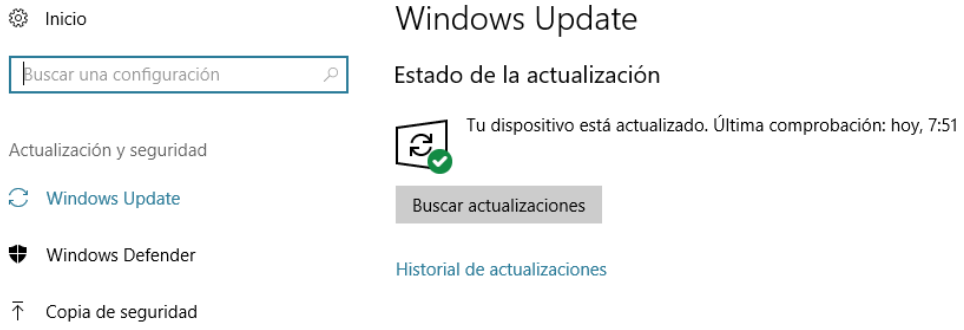
www.cfe.sat.gob

-Desconfía de los ficheros adjuntos, aunque sean de contactos conocidos.



-Asegúrate de que en todas tus cuentas de usuario usas contraseñas robustas.

-Tenga siempre actualizado el sistema operativo y el software antivirus y/o antimalware.



-Evita visitar sitios web de contenido dudoso. Siempre se recomienda mantener actualizados los navegadores web,y al mismo tiempo tener prudencia en nuestras actividades online.