#NoMoreCry #RansomWannaCry5

WANNACRY

Ransomware, una amenaza en constante evolución

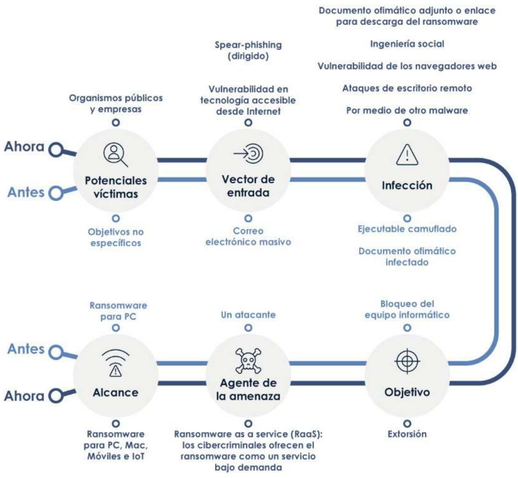
El ransomware de la familia #WannaCry ha sido sin lugar a dudas el más conocido de la historia. Sin embargo, no fue el primero y tampoco el último. Este código dañino marcó un punto de inflexión en el panorama de la ciberseguridad y también en la evolución del ransomware.

¿Qué es un ransomware?

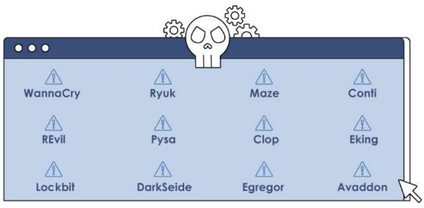
Es un código dañino vinculado al cibercrimen. El objetivo de este ataque es secuestrar los datos y sistemas informáticos de sus víctimas con el objetivo de exigir un pago económico a cambio de recuperar y rescatar la información secuestrada.

Mensaje de un ordenador infectado con WannaCry

Evolución y mejora de las capacidades del ransomware



Los ransomware con mayor impacto en los últimos años



Buenas prácticas para los usuarios frente al ransomware

Disponer de copias de seguridad y actualizarlas de forma periódica.

Mantener los sistemas operativos actualizados.

Emplear contraseñas robustas.

Disponer de antivirus y sistemas antispam.

No utilizar cuentas con privilegios de administrador.

Activar la visualización de las extensiones de los ficheros para evitar ejecución de código dañino camuflado como fichero legítimo no ejecutable.

Disponer de una solución EDR

Buenas prácticas para los organismos y organizaciones

Establecer políticas de seguridad en el dominio. Deshabilitar la ejecución de PowerShell. Deshabilitar la ejecución de macros. Emplear contraseñas robustas. Revisar periódicamente los usuarios con privilegios de administrador.

Establecer políticas de seguridad a nivel de red: Bloquear a nivel de firewall todas aquellas conectividades que no sean estrictamente necesarias.

Disponer de un sistema antispam.

Realizar copias de seguridad de forma periódica.

Mantener el software Y sistema actualizado.

Establecer políticas y medidas de seguridad para los empleados que utilicen sus propios dispositivos electrónicos BYOD (Bring Your Own Device).

Disponer de antivirus y soluciones EDR.

Concienciación de usuarios.

Empleo de bloqueadores de Javascript.

Utilizar el centro de vacunación contra el ransomware del CCN-CERT:

microCLAUDIA

Visita nuestra web