Hacer portada

Ratreo de ciberataques

* Dos días después de la ruptura de las conversaciones diplomáticas entre Rusia y Occidente para parar una invasión a Ucrania, unos 70 sitios web gubernamentales ucranianos sufrieron ciberataques masivos de tipo de denegación de servicio (DDoS). ”. Los "hackers” habían llevado a cabo los llamados ataques "DDos" ("Distributed Denial of Service"), en los que los servidores web eran inundados automáticamente con solicitudes ilegítimas, de modo que la infraestructura de los servidores se sobrecargaba y fallaba.

Solucion:

Detectar el ataque antes de que ocurra. ...

Elegir un buen proveedor. ...

Usar la prevención de ataques DDoS en la nube. ...

Mantener la seguridad en la web. ...

Contar con un buen ancho de banda. ...

Reducir la superficie expuesta a los ataques.

* Las desfiguraciones (defacements) de webs son un tipo de ataque de baja intensidad cuyo efecto puede compararse al de un graffiti. Su impacto reside en lo llamativo de la acción y su impacto psicológico. Otros mensajes en ruso, ucraniano y polaco decían que los datos personales de 43 millones de ciudadanos ucranianos estaban comprometidos, aunque el servicio de seguridad ucraniano lo negó, según AFP.

Solucion:

Limita los complementos de tu página web

Limita los niveles de acceso

Escanea el código fuente de tu sitio

Instala un escáner automatizado de sitios web

* Investigadores de Microsoft descubrieron un programa destructivo dentro de los servidores de agencias ucranianas, un malware conocido ahora como WhisperGate. Simulaba ser un ransomware, pero la contraseña no existía, porque su objetivo en realidad era la destrucción. Expertos citados por el MIT Technology Review señalaron que WhisperGate recuerda a NotPetya hasta en los procesos técnicos destructivos, pero que este ciberataque ha sido menos sofisticado y no estaba diseñado para diseminarse rápidamente.

Solucion:

Actualizacion

Programas de seguridad

A continuación, y aunque sea algo fastidioso, debe crear copias de seguridad de los datos regularmente. Nuestra recomendación es emplear un almacenamiento en la nube que incluya cifrado de alto nivel y autenticación multifactor. Sin embargo, también puede comprar unidades USB o discos duros externos en los que puede guardar archivos nuevos o actualizados

Sentido común

* El parlamento ucraniano denunció la existencia de una campaña de phishing con el objetivo de robar información. En un tuit avisó a los ciudadanos ucrananianos que se están enviando correos electrónicos con archivos adjuntos, y les pide que no abran esos emails porque el enemigo intenta ganar acceso a los dispositivos para obtener información.
* en los ordenadores ucranianos se encontró el llamado software "wiper", un programa malicioso que puede borrar grandes cantidades de datos sin que se note.

Solucion: el sentido común. Hemos visto que este tipo de amenazas, así como casi cualquier otra, suele necesitar la interacción del usuario. Por ejemplo, hacer clic en un enlace, instalar software malicioso, abrir un archivo adjunto por e-mail…

También será interesante contar con programas y herramientas de seguridad. Un buen antivirus puede detectar y eliminar el malware que entre en nuestros dispositivos. De esta forma podremos evitar que nos infecte y pueda llevar a cabo sus ataques para los que fue diseñado.

Una última recomendación y que muchos usuarios pasan por alto es la importancia de tener siempre actualizados los equipos correctamente. Son muchas las ocasiones en las que surgen vulnerabilidades que pueden ser aprovechadas por los atacantes para introducir malware. Debemos instalar los últimos parches de seguridad disponibles. Solo así tendremos realmente seguros nuestros equipos y evitaremos que esos fallos puedan ser explotados.