N&Y MAGAZINE - INFORMATICA A BORDO

http://www.informaticaabordo.com

Informática a Bordo

Nuevas Tecnologías aplicadas en Náutica

CAPITULO 113

CYBERSEGURIDAD PARA EL NAVEGANTE

La tecnología nos persigue a todas partes. El “internet de las cosas” ya es una realidad, y todos vivimos rodeados de objetos conectados a internet, y por tanto vivimos expuestos a la ciberdelincuencia, la nueva forma que tienen los “ladrones virtuales” de hacerse con un botín. Los expertos afirman que la ciberdelincuencia ya mueve más dinero que la droga, y eso es un dato preocupante.

La ciberdelincuencia ya no sólo apunta a las grandes empresas, ni a las medianas o pequeñas. Ahora apunta directamente al usuario, porque han descubierto que es la parte más frágil de la cadena tecnológica.

Las empresas, sea cual sea su tamaño, llevan años invirtiendo en seguridad en todos sus sistemas, activando, mediante hardware y software, barreras perimetrales, antivirus, antimalware y todas las armas de defensa que ayuden a protegerse.

Pero esta mejora en la protección es algo que la ciberdelincuencia tiene en cuenta, y es consciente que cada vez lo tiene más difícil si quiere seguir atacando por esa puerta.
Por otro lado, la parte en la que menos se ha invertido en las empresas es en el usuario, en su formación y conciencia para no ser el punto más débil de la cadena. Por mucho dinero que invierta la empresa en seguridad, si el usuario no tiene conciencia y no es formado en estos temas, se convierte en la puerta de entrada más fácil de derribar para los ciberdelincuentes.

¿Porqué afecta también al entorno náutico?

El entorno náutico es como cualquier otro. Tenemos el barco lleno de tecnología, como en casa o como en el trabajo. La electrónica que tenemos más antigua está desconectada de internet, pero a medida que nos renovamos o equipamos, comenzamos a incorporar electrónica que ya tiene conexión a la red, por cable, wifi o 4G.
Desde el momento que un objeto está “conectado”, ya es un objeto alcanzable, y por tanto atacable. Es un punto más de entrada para el ciberdelincuente.
Por ejemplo, si instalamos un cargador de baterías que nos ofrece una APP para monitorizarlo o actualizarlo, ya tenemos le estamos dando al hacker una puerta para llegar a dicho cargador. Y nos preguntamos ¿qué le importa a un hacker llegar a mi cargador? No le importa nada, pero para ellos es como un

“videojuego”. Los objetos alcanzables y “derribados” son puntos en su juego virtual. Es un reto que consiste en destruir e infectar hasta donde lleguen.

Lo más preocupante es que este deporte de infección ha encontrado una forma de financiarse. Ahora llegan, infectan, destruyen, pero dejan una cerradura de la que sólo ellos tienen llave para volver al estado normal, y nos piden un rescate. Y esa llave virtual es tan compleja que sólo el que la cierra tiene opción de abrirla.

¿Cómo pueden fastidiarnos a bordo?

En vacaciones seguimos dependiendo del móvil, del portátil y de las comunicaciones para seguir en contacto con el mundo real y con el trabajo.

Si en una empresa el usuario es atacado, estará en un entorno que puede ser ayudado por el informático local, con las herramientas necesarias para subsanar el problema, en caso de estar a tiempo. Pero si nos atacan en plena navegación o en nuestras vacaciones, no dispondremos de esas manos y herramientas que nos ayuden a recuperar el sistema o la conexión con la electrónica. Cargadores, sensores, cámaras, cartas náuticas, electrónica … todo puede quedar inaccesible, o incluso bloqueado.

Y también podemos sufrir un ataque directo a los datos del móvil o el portátil y secuestrarnos la información. En ese caso dudo que tengamos recursos a bordo para recuperar los equipos o la información atacada.

El ataque más temido actualmente es el crytolocker. El ataque producido por este ramsoware nos deja toda la información en manos de un chantaje cuya única solución, si no tenemos un buen plan de recuperación, es el pago ilegal a los hackers de una cantidad elevada de bitcoins, que va aumentando a medida que pasan los días.

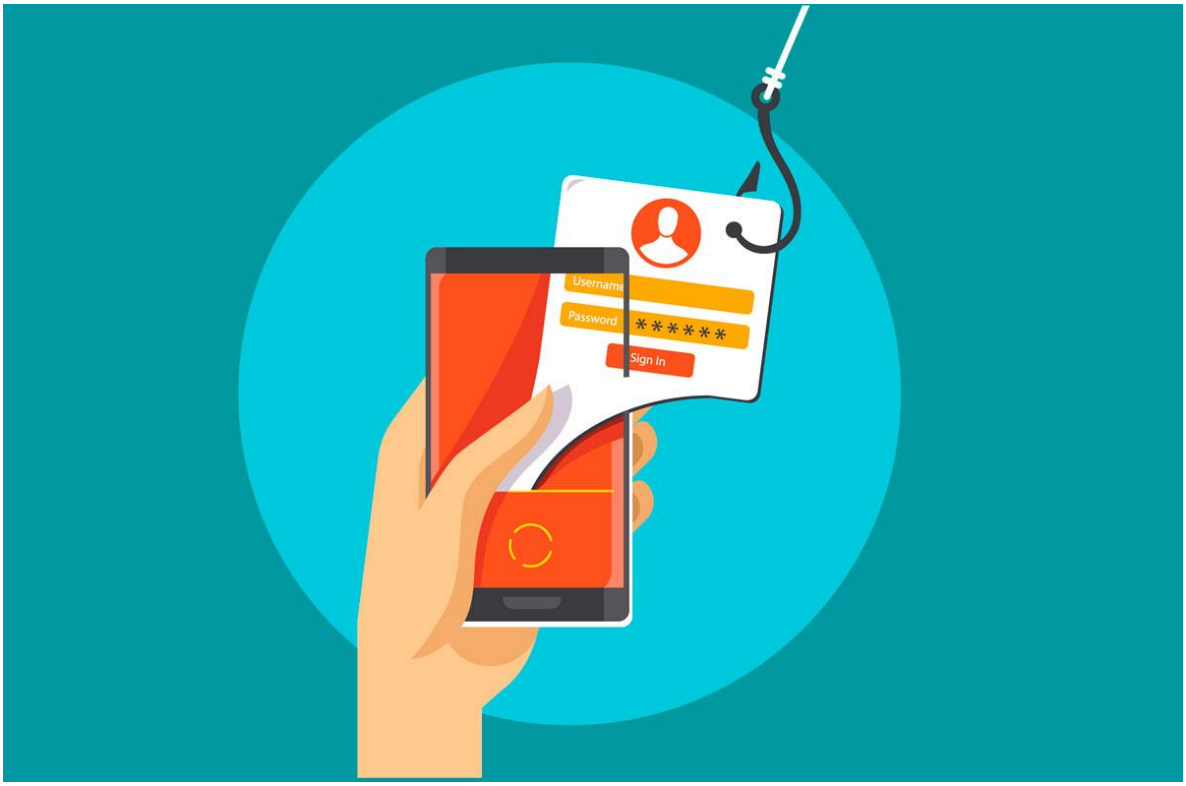
¿Qué es el ransomware y cómo ataca?

El malware (virus, troyanos…) es un software que infecta y manipula el sistema. Ransomware se forma al unir ransom (rescate, en inglés) con ware (producto o mercancía, en inglés). El ransomware es un malware que cifra archivos, solicitando un rescate para recuperar su acceso.

La entrada más habitual: Phishing

Hasta ahora era habitual recibir ataques por la vulnerabilidad de la seguridad perimetral de las empresas, pero ahora han redirigido sus fuerzas directamente hacia los usuarios con métodos de phishing para entrar en los sistemas e infectarlos.

El phishing consiste en engañar a un usuario haciéndole creer que está ingresando a un sitio seguro que ya conoce, para llevarle a otra dirección con la misma apariencia, con el afán de que el usuario entregue sus credenciales y exponga su información a los atacantes.



El phishing tiene tres componentes:

- Ataque: Se realiza mediante un correo electrónico o una llamada de teléfono
- Atacante: Se hace pasar por una persona u organización de confianza
- Objetivo: Obtener información personal confidencial

El atacante busca estos objetivos:

- Nombres de usuario y contraseñas
- Números de la Seguridad Social y de cuentas bancarias
- Números de tarjetas de crédito y de identificación personal (PIN)
- Fecha de nacimiento, datos de familiares
- Otros datos de interés para crear diccionarios de contraseñas

¿Qué hacen cuando ya nos han cazado?

Una vez han entrado en uno de nuestros equipos estudian si somos una presa de la que pueden sacar algo, o bien nos utilizan de salto para llegar a otra más rentable. Y lo hacen sin dejar rastro, porque son auténticos profesionales.

- Estudian hasta dónde pueden llegar con los accesos logrados
- Recopilan datos de acceso a cuentas de correo, bancos, tarjetas …
- Identifican a los usuarios que realizan pagos o reciben facturas
- Localizan las copias de seguridad, accesos, periodicidad
- Copian las bases de datos de contactos para conseguir más víctimas
- Crean filtros en las cuentas de correo para desviar pagos y avisos
- Encriptan para pedir recompensas

Formación y conciencia para el navegante usuario de tecnología

La formación y conciencia del usuario hoy en día es más importante que las medidas que podamos tener con firewalls, antivirus o cualquier otra medida de protección.

Estos son algunos de los consejos que debemos seguir los usuarios.

Evitar ser víctimas de engaños

- No abrir correos de usuarios desconocidos o que no hayamos solicitado
- Revisar los enlaces antes hacer clic, aunque sean de contactos conocidos
- No contestar correos solicitando borrado de la lista, ya que indicamos que estamos “vivos”
- No seguir enlaces acortados (Ejemplo: https://by.did/ghr/….)

- No abrir ficheros adjuntos que no esperemos, aunque sean de contactos conocidos
- Desconfiar de los mensajes que nos pidan datos o que nos pidan una acción ante una posible sanción

¿Cómo puedo protegerme?

Además de estar muy atento …

- Tener siempre actualizado el sistema operativo de nuestro ordenador, móvil, tableta …
- Tener actualizado y activo el antivirus y antimalware
- Utilizar contraseñas robustas (8 dígitos, mayúsculas, minúsculas, símbolos)
- Utilizar MFA (autenticación multi-factor) para todo, comenzando por el WhatsApp

Y si cumplo todas las recomendaciones, ¿puedo infectarme?

La respuesta es SÍ, a fecha de hoy no existe "vacuna" preventiva, ni se espera, por lo que la atención, conciencia y sentido común del usuario son la mejor vacuna.

Primer paso, proteger nuestro WhatsApp

La APP de WhatsApp incluye una funcionalidad de verificación en dos pasos para evitar que nos lo capturen y nos roben datos. Para activar esta verificación necesitaremos tener WhatsApp ya configurado en nuestro móvil,

pensar una clave numérica de 6 dígitos y disponer de una cuenta de correo (para recuperación de la clave dígitos en caso de pérdida)

1. Vamos a «Configuración» (rueda dentada abajo a la derecha)
2. Entramos en «Cuenta»
3. Entramos en «Verificación en dos pasos» y «Activar»
4. Nos solicitará un código numérico de 6 dígitos, 2 veces para confirmar
5. Nos solicitará una cuenta de correo de recuperación
6. Guardar los cambios o «Ok»

La cuenta de correo es muy recomendable ya que en caso de olvidar el código de 6 dígitos podremos restablecerlo a través de esta cuenta de correo. De lo contrario, tendremos que esperar 7 días a recuperar acceso a nuestro WhatsApp.

Si no queremos que un hacker nos fastidie las vacaciones tenemos dos opciones. La mejor protección es dejar el móvil y el portátil en casa, pero si no somos capaces, siempre podemos tener conciencia y echar mano del sentido común.

José María Serra Cabrera
Capitán de Yate
Licenciado en Informática
Gerente DEINFO Servicios Informáticos