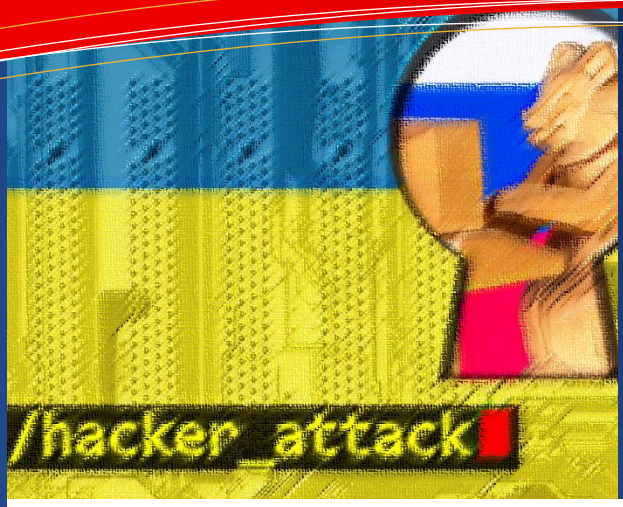
Volúmen
03
Marzo
2022

BARTIZAN SECURITY

Revista Mensual de
Tecnología
Informática

BartiTimes



En esta edición

¿Se sale de control? P.1

Cómo te espian P.2

¿Quién nos salva ahora? P.3

¿Por qué es tan fácil para ellos?

Obtener información es bien fácil y rápido en el Internet. Dedicar tiempo a la búsqueda y organización de datos se puede hacer de forma efectiva. Solo se necesita una computadora, acceso a la Internet y un objetivo. La búsqueda no es complicada ni intensa. Por ejemplo, teniendo acceso a una cuenta de Facebook que no esté protegida, se puede lograr acceder todas sus interacciones, y las mismas dan su localización, su número de teléfono (gracias a WhatsApp), a sus fotos, a su Instagram, a su Twitter o algúna otra red que use el mismo email de registro.

La necesidad

La necesidad de protegerse es inminente ante la facilidad de robar sus datos personales aludidos. Ejemplo de herramientas que pueden ayudar son:

1) Manejador de contraseñas
2) Protector de perímetro (Firewall)
3) Servicio de VPN
4) Codificar su correo electrónico
5) Seguridad de la computadora (EDR)
6) Artefacto con 2FA

LEER MAS

Ucrania, Rusia y Estados Unidos, ¿se sale de control la guerra cibernética?

Podemos decir que el mundo está interconectado por completo a través de las redes del Internet. Lo que antes se consideraba lejos -geográficamente hablando- ahora se encuentra a milisegundos de conexión gracias al Internet. Por esta razón es que podemos decir que la guerra entre Rusia, Ucrania y los Estados Unidos, impacta al mundo entero. Es evidente que la manera política de atacar el problema es aplicando sanciones para asfixiar la economía de Rusia.

El problema principal que trae este método, es que despierta vectores nuevos de ejecutar ataques para recuperar el dinero perdido y a su vez encontrar formas costo efectivas de atacar. He aquí donde despierta la guerra cibernética. Hemos comentado anteriormente que en el 2021, se reportaron las cifras más altas de pérdidas monetarias por los ataques de “ransomware” y “phishing”. La peculiaridad es que en vez de ser ataques efectuados por cibermaleantes, ahora veremos naciones ejecutando este tipo de ataques, de una manera más sofisticada y directamente con la meta de adquirir dinero fácil invirtiendo bien poco en el proceso.

Esto significa que todo el que esté conectado al internet tiene el potencial de convertirse en una víctima de dichos ataques. Ucrania siempre ha sido la “chata” de Rusia cuando se trata de ataques cibernéticos. Ahora, como Rusia está desesperada económicamente, los ataques serán contra todo lo que se mueva en el Internet que les permita recuperar dinero.

No se sorprenda, esto no es nuevo. Rusia lleva atacando activamente a los Estados Unidos desde hace mucho tiempo. Precisamente los ataques del 2020, usando SolarWinds y el ataque más reciente al Colonial Pipeline, fueron los últimos dos que colmaron la copa y despertaron a los Estados Unidos. Ahora el presidente Biden está más exigente y activo en exigir y lograr cumplimiento a las empresas que hacen negocio con el gobierno.

En medio de este proceso, no sólo está la gente de Ucrania sufriendo, sino todos aquellos que llevan a cabo negociaciones y transacciones internacionales. Todo aquel que haya sufrido las consecuencias de un ataque de ransom y todo aquel que no está preparado, recibe su agüita de los ataques cibernéticos.

¿Como protejo mi artefacto movil?

No hay que ser el más tecnológico para proteger tus artefactos móviles. Solo necesitas estar consciente de lo que tus aplicaciones pueden hacer y aprender a configurar los accesos a los que das permiso a tu aplicación para accesar.

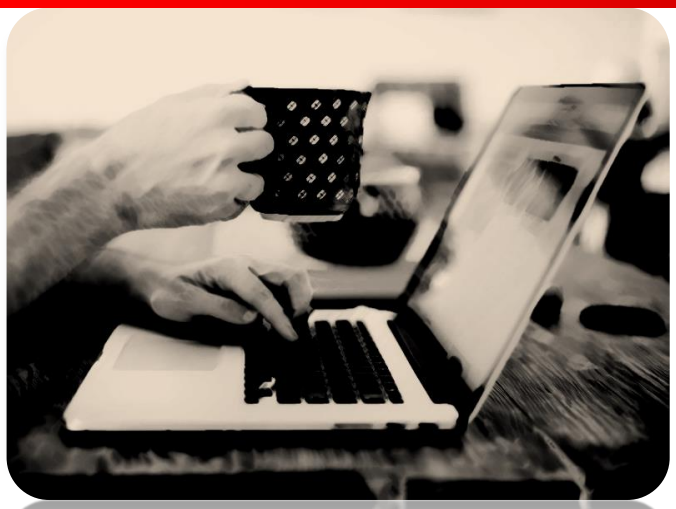
Lo básico que puedes hacer:

- Ponerle un PIN de más de 4 números
- Biometría = tu dedo o tu cara
- Usar VPN para el Internet
- Solo descargar aplicaciones oficiales de la tienda de aplicaciones, que estén actualizadas
- Hacerle “BACKUP” a tu teléfono frecuentemente
- Aprender cómo borrar o asegurar tu artefacto remoto en caso de pérdida.
- Borra aplicaciones viejas que no uses y mantén actualizadas las que tienes instaladas.
- No uses WIFI públicos, a menos que tengas un buen servicio de VPN
- Apaga el “autocomplete” o “autocorrect”
- Habilita y confugura la aplicación para encontrar tu artefacto remotamente (en caso de pérdida)
- Si eres dueño de un negocio, debes considerar usar Yubico como 2FA para tu artefacto.

Recuerda que el sistema es tan fuerte como la persona que lo usa y lo configura. Siempre el punto más débil de todo equipo electrónico, es la persona que lo usa. Si tus prácticas de seguridad son pobres, la facilidad de poder atacarte es mayor.

En Bartizan Security estamos para ayudar. Escríbenos por Whatsapp si interesas orientación.

Bartizan Security
WhatsApp Business Account



Como es que los cibermaleantes te espían.....

Aumenta el nivel de intensidad de los ataques cibernéticos, victimizando a todos los civiles que estemos conectados al Internet.

Es un arte obtener información de un artefacto electrónico. Si analizamos la situación con malicia; ¿Qué artefacto abunda más en el Internet y que contiene millones de datos personales? ¡Exacto, los artefactos móviles!

Este mes de marzo se disparan las vulnerabilidades de 0-días o mejor conocidas como vulnerabilidades que todavía no tienen parchos para corregirlas. Al no tener parchos del manufacturero, o del desarrollador que preparó el programa, estas vulnerabilidades corren el riesgo de que cualquiera las pueda utilizar para ganar acceso a tu artefacto móvil. No importa cuán fanático usted sea con su artefacto móvil; tanto Apple IOS, como Google Android, tienen el mismo problema. Se gana acceso tan fácil como:

1. Un enlace que te envíen por Whatsapp, o por FB Messenger.
2. Algún correo electrónico que abras desde tu artefacto móvil,
3. Simplemente un texto con una foto con enlace,
4. **5.** Una llamada desde un teléfono clonado (duplicado para hacerse pasar por un familiar) y te atraparon.

Si eres el objetivo de un “cibermaleante”, ellos explotarán las multiples posibilidades de ganar acceso a tu artefacto móvil.

> “ellos explotarán las múltiples posibilidades de ganar acceso”

Una vez logran tener acceso a tus artefactos ya comprometidos, es hora de comenzar a husmear en el mismo.

Detrás de la interfase gráfica que tienen los sistemas operativos de los artefactos móviles, existe un directorio de archivos por el que se puede navegar igual que una computadora. Cada directorio almacena datos de las aplicaciones instaladas y los mismos almacenan toda tu información personal que en algún momento has ingresado en este.

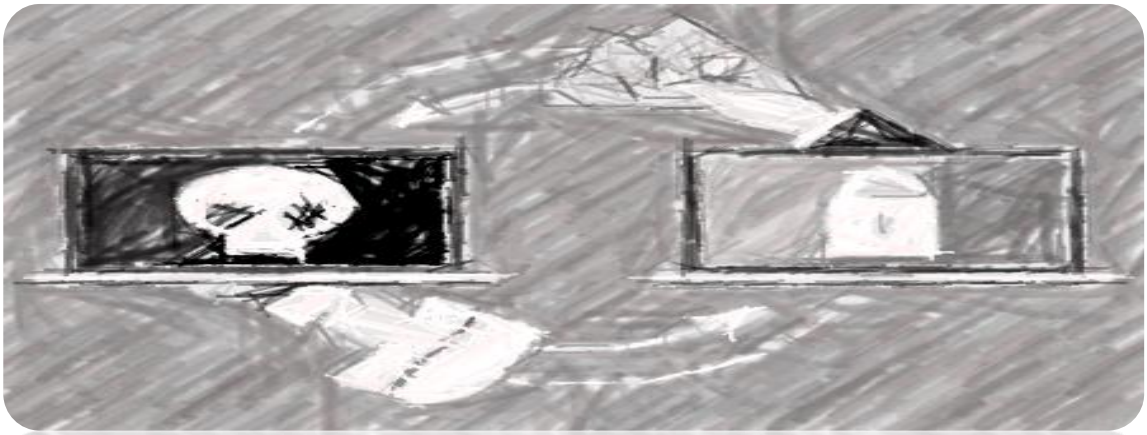
Una vez el cibermaleante está dentro de estos archivos, podrá obtener la información necesaria para preparar un plan de ataque. Ya sea instalar un “ransomware”, extraer información para extorsionar a tus familiares, o si eres el objetivo de alquien, obtener tus secretos escondidos en el artefaco móvil. Este tipo de ataque es más común de lo que la gente piensa y no necesariamente tiene que ser un cibermaleante. Esposos o esposas, novios o novias celosas, pagan mucho dinero a expertos en estas artimañas para obtener la información.

¡Agúzate que te están velando!

Si te preocupa este fenómeno, debes sacar un rato para configurar las aplicaciones que tiene tu dispositivo móvil y limitar los accesos que tiene cada aplicación a las funciones críticas de la unidad móvil. Cada aplicación se puede configurar de manera individual. Todas -por configuración de fábrica cuando se instalan- tienen acceso a:

- **Cámara / tus fotos**
- **Micrófonos / Bluethooth**
- **Tus contactos**
- **GPS / servicios de localización**
- **Micrófono**
- **Internet**
- **Data Celular (a los que apliquen)**
- **Analizar tus pasos**
- **Notificaciones**
- **Inteligencia Artificial (Alexa, Siri)**

Dale acceso sólo a lo que necesitas de la aplicación.



Ciber Secuestro: mejor conocido como Ransomware

Cada día que pasa se reporta que los ataques de ransomware son abundantes y, aunque sean reportados en las noticias, la prensa y la televisión, es lamentable tener que escribir que, a marzo de 2022, todavía no estamos listos para mitigar este problema.

Nuestra cultura de dejarlo todo para ultima hora, o “eso no pasa aquí”, nos lleva a tener un sentido falso de seguridad. Cuando nos toca recibir el ataque, no estamos listos. Lo peligroso de eso es lo facil que se le hace al cibermaleante secuestrar todos nuestros datos.

El cibermaleante siempre busca un punto de entrada a tu computadora, usando -no solo vulnerabilidades en la misma- sino también analizando el comportamiento del usuario de la computadora en su uso diario. Analizando tu tráfico en el Internet (el cual viaja en pleno texto) se puede ver de donde viene la informacion y hacia donde se dirige. De aquí los cibermaleantes pueden planificar cuál es el punto fácil de atacar de una persona. Su preferencia de carros, su afán por ver mujeres en bikini, porno, obsesión por los gatos, compras por Amazon, búsquedas en Clasificados Online, comportamientos en Youtube, servicios de “streaming”, artefactos de Gaming (Xbox, PS5) y comportamientos en las redes sociales. Pedazos de información capturados en el Internet cuando se juntan para análisis, les da a estos maleantes un marco completo de las posibles oportunidades de ataque.

El mejor consejo es estar atento, ser cauteloso con los correos electrónicos, tener “backup”, obtener algún tipo de dispositivo de seguridad de perímetro (firewall), NO TENER TODOS LOS HUEVOS EN UNA CANASTA, hacer “backup” usando múltiples fuentes de “backup”. Finalmente, estar alertas a eventos recurrentes de solicitudes de ayudas económicas para remisiones hacia Ucrania. El impostor puede crear un (scam) esquema que aparente ser legitimo para “ayudar”, pero en realidad el mismo te lleva a un enlace cuya intención es atrapar tus artefactos electrónicos.

Consejos de Tecnología del Mes

Q: ¿Puedo cifrar mis correos de GMAIL?

A: ¡Si! Existen varias alternativas para cifrar tu correo electronico en GMAIL. Si tu negocio usa GSuite, sólo tienes que ir a configuracion de seguridad y hacer los ajustes necesarios para lograr cifrar tu data en tránsito de un lado a otro en Gmail. En el mundo de la informática, las ofertas de cifrado que ofrece Gmail por defecto no se consideran muy seguras y esto da oportunidad a que tus datos sean cifrados, pero definitivamente es mejor que nada. Si estas buscando una alternativa más fuerte, añade PGP en GMAIL.

Pretty Good Privacy conocido como PGP, es un algoritmo de cifrado que incorpora buenos elementos de seguridad comunmente utilizado en protocolos de correos electrónicos. Extensiones para Chrome como FlowCrypt permiten utilizar PGP en GMAIL Esto ofrece una capa de protección que nos ayuda a cifrar los correos esto cifra el contenido para que el mismo no viaje en pleno texto por el internet, dando una capa de seguridad adicional a los datos que viajan en tu correo electrónico.

Ciberseguridad

¿Cómo protejo mi negocio del secuestro cibernético?

Proteger tu negocio de un ransomware no es tedioso, pero requiere estar atento y de la participacion de todo el personal en la organización. Es importante:

- Fomentar una cultura de ciberseguridad en la organización
- Enfatizar al personal incluyendo su liderazgo, que ciberseguridad no es sólo informática sino toda aquella persona que interactúa con la informática
- Constante capacitacion sobre la tecnologia y cómo la empresa utiliza esta tecnología, poniendo énfasis a posibles vectores de ataque en la organización
- Desarrollo de politicas de seguridad con enfoque a proteger la data de la organización y capacitación sobre estas politicas específicas en la organizacion

Aplicación del Mes

Degoo

Se dice que si no pagas por el producto, es por que tu eres el producto. Es práctica común, pensar en Dropbox cuando hablamos de almacenamiento en la nube. Degoo ofrece una gran alternativa a Dropbox. Tu data almacenada es cifrada. La oferta gratis incluye 100GB de almacenamiento, conexión de hasta 5 artefactos y programa de referido donde te aumenta la capacidad cuando refieres a compañeros. ¡Siempre es bueno tener alternativas!

Desarrollo Profesional

Manejar proyectos es crucial en el mundo de la informática. Todo en la informática es sensitivo a tiempo. Es importante saber como manejar las tareas y poder identificar prioridades. Aprender de PM (**Project Management**) te ayudará.

Eventos

- **Simposio de Cumplimiento/Fraude, Derecho Cibernético y Ciberseguridad para dueños de negocios.**

Estamos organizando un simposio donde convocaremos e integraremos abogados, oficiales de cumplimiento, expertos en Ciber Seguridad, expertos en sistemas de información y analistas en alineamiento de estrategias de informática. **Tan pronto el COVID y las órdenes gubernamentales nos permitan,** informaremos la fecha, hora y lugar. Este evento estará enfocado en ayudar y apoyar a los dueños de negocios y personas que trabajan por cuenta propia. No importa el tamaño de tu negocio o de tu operación, es importante entender cómo alinear las estrategias en el uso adecuado de la tecnología, como negociar un Ransomware, cómo capacitar a tus empleados, cómo prepararse para un desastre cibernético, derecho cibernético y tu empresa, cumplimiento legal y ciberseguridad bajo el enfoque en la nueva directriz del presidente Biden.

El Simposio será una oportunidad para conversar y crear enlaces donde juntos podremos encontrar soluciones para cada posible situación. Estaremos anunciando más detalles por nuestra página de Facebook https://www.facebook.com/BartizanSec .

BARTIZAN SECURITY

Puerto Rico
787.903.5034
www.bartizansecurity.net