Protégete ante el Ransomware

Publicado el El Informatico - 1 de septiembre de 2021 -

El ransomware es un tipo de malware que encripta la información de tu dispositivo, y/o que toma el control del mismo, para después pedirte un rescate por su recuperación. Normalmente en forma de criptomonedas para intentar evadir la trazabilidad del pago.

En éste artículo te explico algunas de las medidas que puedes tomar para evitar éste tipo de ataques (y en general, cualquier tipo de *malware*) y evitar así que se te atragante la vuelta al trabajo.

1. Haz copias de seguridad de todos tus archivos y datos diariamente.

Esto es algo que no debería de tener ni que decir. Sin importar que nos infectemos con un cryptolocker o que nuestro disco duro "*explote*", podemos sufrir una pérdida de información en cualquier momento y por cualquier motivo. Por ello es de vital importancia realizar copias de seguridad de todos los datos que sean de importancia. A ser posible, de forma diaria. Así en el peor de los casos, sólo perderás

unas horas de trabajo. Estas copias de seguridad deberían almacenarse en un dispositivo externo. Por ejemplo, un disco duro externo, un NAS, o algo tan simple como una memoria USB. Y si es posible, en varios dispositivos a la vez.

Una copia de seguridad puede ser un simple copia-y-pega de los archivos, pero si necesitas un mayor control sobre dichas copias existe multitud de software e incluso servicios para ello. Desde opciones de pago como Acronis a opciones de código libre como UrBackup o Bacula, entre muchos otros.

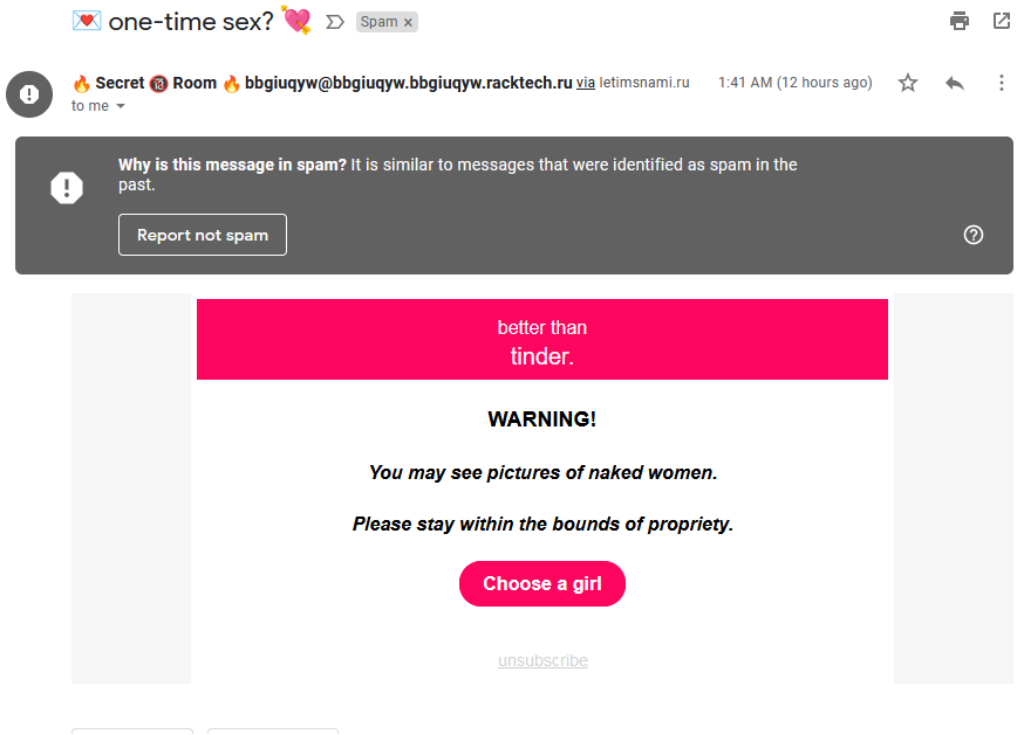
En el caso de que sufras una pérdida de datos, siempre podrás acudir a éstas copias de seguridad para restaurar tus datos, una vez hayas solucionado el problema.

Recuerda que si dispones de información sensible como datos gubernamentales o información importante sobre tu empresa, deberás además encriptar el medio donde almacenes tus copias de seguridad. Bien usando LUKS (En Linux) o bien usando BitLocker o similar en Windows.

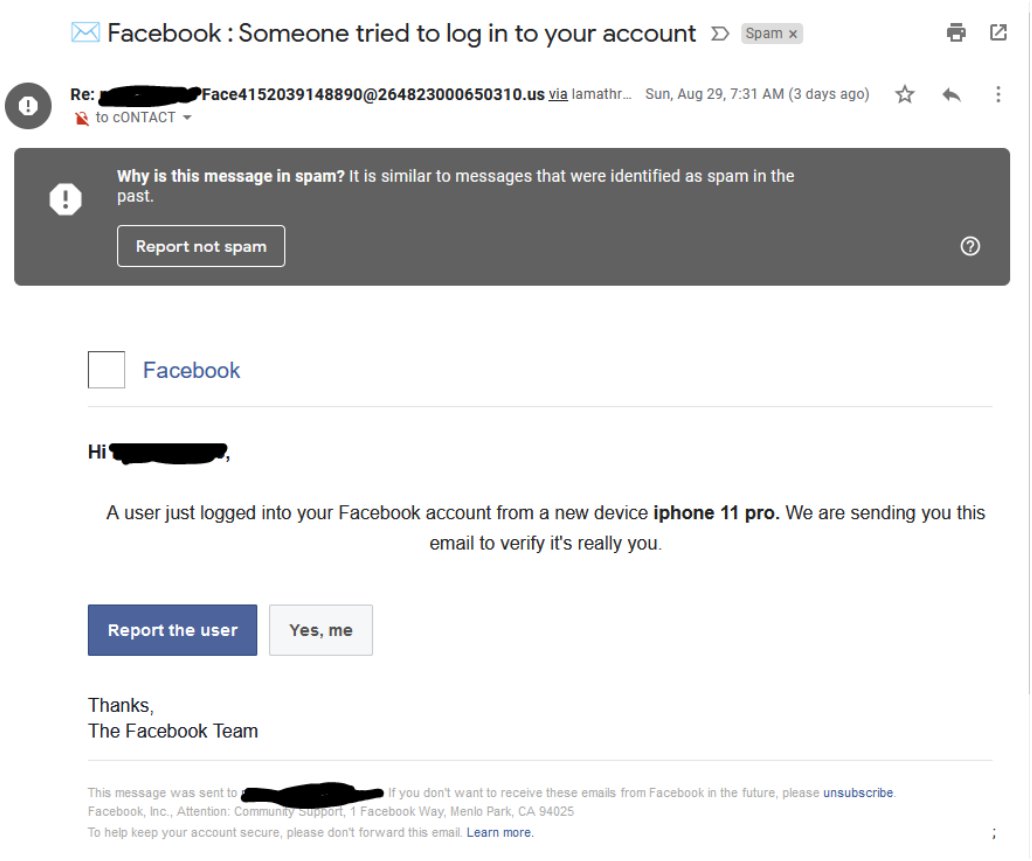
2. Reduce los vectores de ataque al mínimo

Lo mejor es siempre evitar infectarse con éste o cualquier tipo de malware, y por ello es necesario tomar precauciones. Normalmente cualquier malware se propaga por correo, o por descargas de internet de sitios fraudulentos. Y una vez infectado un equipo, se propagan por la red aprovechándose de diferentes vulnerabilidades en los servicios y protocolos de la misma. Por ejemplo, mediante vulnerabilidades en el sistema de impresión de Windows, o incluso en los propios servicios de Microsoft.

En el caso de los correos electrónicos, en muchos casos son fáciles de identificar ya que provienen de fuentes extrañas y contienen enlaces raros que no llevan al sitio que sugieren o que simplemente se ve al kilómetro que son correos maliciosos.



Ejemplo típico de correo malicioso, detectado automáticamente por GMail como tal. En éste caso es demasiado obvio que se trata de un correo malicioso.



Ejemplo de un correo malicioso suplantando a Facebook. ¡Ojo a la dirección del remitente! Aunque el contenido del mensaje es bastante creíble (excluyendo algunas incongruencias en la redacción del mensaje) la dirección delata que se trata de un impostor.

Pero en ocasiones no puede estar tan claro, **llegando a veces incluso a copiar el formato interno de los correos de tu empresa en el caso de ser un ataque dirigido a la misma**.

Por éste motivo, todas las comunicaciones por correo electrónico en la empresa deberían de estar firmados y cifrados usando PGP o similar. De éste modo, y si se usa correctamente, un atacante no podrá suplantar la identidad de un empleado de tu empresa, ya que no poseerá la firma electrónica, ni podrá inyectar código malicioso en el mensaje al estar cifrado.

Si estas usando PGP y recibes un correo sin cifrar, aunque sea de un contacto de confianza, simplemente **no lo abras** y desconfía del mensaje. Contacta con el remitente de forma inmediata para esclarecer si ha podido haber un error, o si es un intento de ataque.

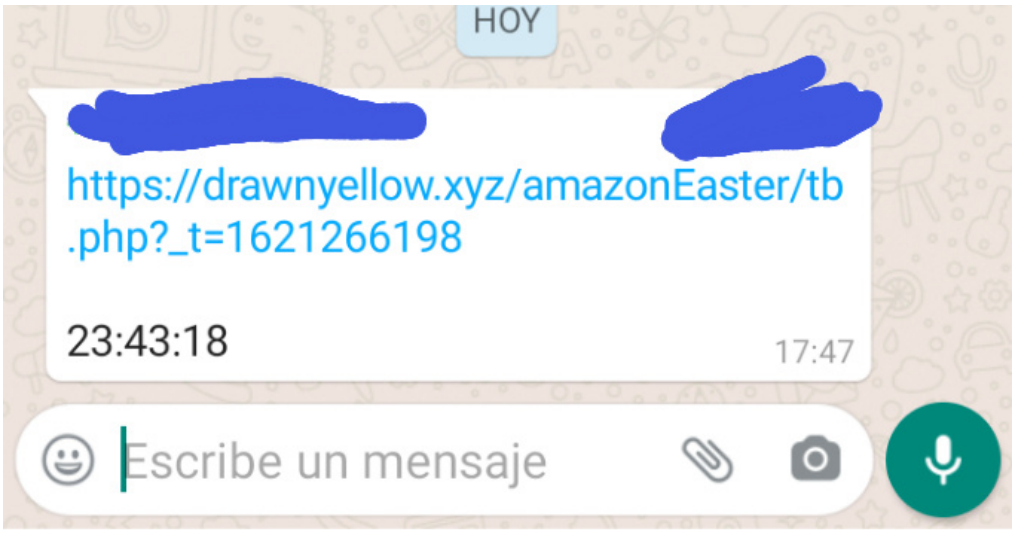
3. No descargues NADA que no sea de ninguna fuente de confianza.

No tengo mucho que explicar sobre ésto, porque ya redacté un artículo mostrando

cómo una página maliciosa podría hacerte descargar malware. Muchas veces al realizar descargas se nos ofrece una **firma de verificación** para asegurar que nadie haya interceptado la descarga e inyectado código malicioso en la misma.

Descarga siempre de fuentes de confianza y asegúrate siempre de que los sitios web desde los que descargas contienen un certificado SSL válido para cifrar la comunicación. Si estás en el ordenador de una empresa, consulta a tu departamento de IT si fuese necesario.

4. Ojo a los enlaces por chat.



Enlace potencialmente sospechoso en una conversación por Whatsapp.

El Whatsapp es también un potencial vector de ataques, y hay muchas empresas que les dan teléfono móvil a sus empleados. Si eres un trabajador que posee un teléfono de empresa, deberás cuidar también que nadie pueda atacar el mismo (Y si no pero igualmente dispones de smartphone, también, por supuesto).

Al igual que con los correos electrónicos, los mensajes de whatsapp (o cualquier otro servicio de mensajería instantánea) pueden contener enlaces maliciosos, incluso de personas en tu lista de contactos que hayan podido infectarse.

Recuerda que, en ocasiones, éstos mensajes pueden resultar poco sospechosos a la vista, pudiendo incluso suplantar a tus contactos para ganarse tu confianza.

5. Mantén tus sistemas actualizados.

En la práctica, en un entorno de empresa, es a veces es complicado realizar actualizaciones precisamente por motivos de seguridad y de integridad. Pero es necesario, ya que a veces se ofrecen parches para vulnerabilidades críticas que podrían abrir paso a cualquier malware para infectar todos los equipos de la red.

En el caso de equipos domésticos ésto es más sencillo. En el caso de Windows incluso el propio sistema te fuerza a actualizar de forma periódica. Algo que a todos

los usuarios nos trae quebraderos de cabeza en ocasiones, pero que en cierto modo es necesario.

¿Es conveniente usar un antivirus?

Los antivirus no son infalibles y existen muchas piezas de malware que, o bien no son conocidos y no están en la base de definiciones del antivirus, o no puede ser detectado de ningún modo porque utilizan mecanismos para ocultarse que son lo suficientemente sofisticados como para engañarlos. Por eso lo mejor es siempre la **prevención**.

No obstante, siempre puede ser conveniente usar alguna herramienta anti-malware para al menos intentar evitar la entrada de lo que sí es conocido y se puede detectar. Windows incluye, al menos en las ediciones domésticas, una suite de seguridad llamada Windows Security. Esta suite incluye un servicio de detección de malware en tiempo real (centinela) además de la posibilidad de realizar un escaneo sobre tus unidades. No obstante, si no confías en este servicio, siempre puedes acudir a servicios de pago como Malwarebytes o cualquier otro similar.

¿Y si uso Linux?

Usar Linux o cualquier sistema similar, como FreeBSD, está muy bien. Pero no te hace invulnerable a ningún ataque. El ejemplo más obvio está en los dispositivos Android, cuyo núcleo es Linux (Si bien Android no es un ejemplo a seguir en el tema de seguridad y privacidad). Muchos centros de datos y empresas utilizan sistemas basados en Linux como Red Hat Linux o CentOS que también han sufrido ataques en el pasado.

El mito de que Linux "no tiene virus" es un mito que se basa en la "seguridad por oscuridad" (security by obscurity), que sugiere que un sistema no puede ser atacado si el atacante desconoce de su existencia o funcionamiento interno, o en éste caso por la falta de interés por parte de los posibles atacantes debido al bajo número de usuarios. En el mundo de la seguridad informática éste principio está completamente desmentido. Precisamente una buena parte del "hacking" consiste en descubrir y estudiar éstos sistemas para su explotación. Y en el caso de Linux, es bastante popular en la actualidad ya que hay infinidad de dispositivos como servidores, routers, domótica, Android TV, etc, cuyo sistema está basado en Linux y cuyos sistemas son explotados a diario para hacerse con el control de los mismos.

No pagues nunca el rescate

Si has seguido el punto 1 (el más importante), formatea todas las unidades de disco del equipo, reinstala el sistema operativo y restaura tus copias de seguridad. **No pagues nunca por el rescate de tus datos**, no es seguro que te devuelvan tus

datos (personalmente, si fuese un pirata informático, me llevaría el dinero sin más) y lo que es peor, estarás alentando a que el atacante siga haciendo lo que hace. Que cada vez éste tipo de ataques sean más comunes **es en parte porque las víctimas pagan por el rescate**.

ANTERIOR

Mantén tus contraseñas seguras

SIGUIENTE

Houston, tenemos un problema energético en Europa... y es grave.

Buscar ...

Entradas Recientes

- El Metaverso: Nada nuevo en el horizonte
- Estafas telefónicas: ¡No caigas en la trampa!
- Jueves de buenas noticias
- Facebook, una vez más, en problemas. Y es su propia culpa.
- Si usas Twitch, cambia tu contraseña de inmediato
- Diferencias entre Internet y La Web. ¿Qué es cada uno?

Categorías

Actualidad | Android | Básicos | Ciberseguridad | Criptografía | Emulación / Virtualización | FOSS | Hacking | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS