Ciberseguridad aplicada al Coronavirus

La sociedad está viviendo una situación inusual a raíz de la pandemia provocada por el coronavirus SARS-CoV-2 (popularmente conocido como COVID-19) y que ha causado una disrupción sin precedentes en el mundo, la cual se ve reflejada en el temor generado por el cierre de negocios y colegios, la prohibición de viajar, la dificultad de conseguir algunos productos en supermercados y por el impacto en el mercado financiero.

Como era de esperarse esta situación de alarma social está siendo aprovechada por los ciberdelincuentes para realizar campañas fraudulentas explotando las vulnerabilidades que se generan al implantar mecanismos, en algunos casos improvisados, para habilitar el trabajo remoto o la necesidad en los hospitales de obtener información de forma rápida para la gran cantidad de pacientes que están teniendo que atender en muy poco tiempo, evidentemente con el objetivo de extorsionar a las víctimas.

Por ejemplo, este correo con un malware adjunto suplantando la identidad de la Organización Mundial de la Salud (OMS), está siendo utilizado para engañar a los receptores del mismo para descargar un fichero con supuesta información de referencia con medidas de seguridad frente al coronavirus:

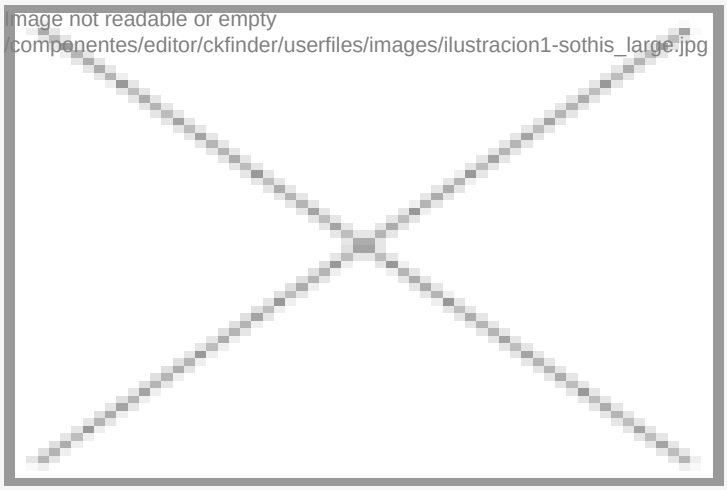

Ilustración 1: Ejemplo de suplantación de identidad a la Organización Internacional de la Salud.

El problema no se queda aquí, también están aprovechando los ciberdelincuentes para explotar vulnerabilidades e introducir ramsonware en centros hospitalarios, provocando inestabilidad en sus sistemas informáticos e impidiendo a los mismos atender de forma óptima las necesidades de los pacientes, exigiendo un rescate para recuperar el control de los datos.

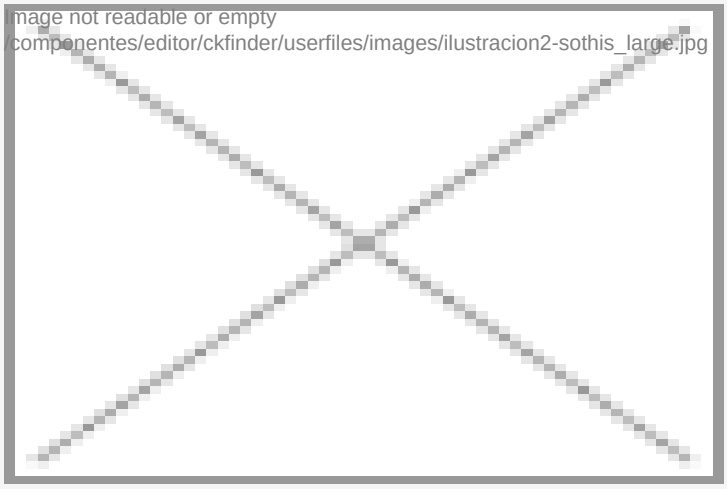

Ilustración 2: Hospital Checo víctima de un ciberataque en pleno brote de COVID-19

Uno de los malwares más activos que utiliza al coronavirus como anzuelo es Koadic, que mediante un correo electrónico adjunta una hoja de cálculo con el nombre de “Test result of medical analysis” que, al ejecutarse, infecta el dispositivo consiguiendo acceso a información sensible como credenciales de nuestras aplicaciones o de nuestra cuenta bancaria.

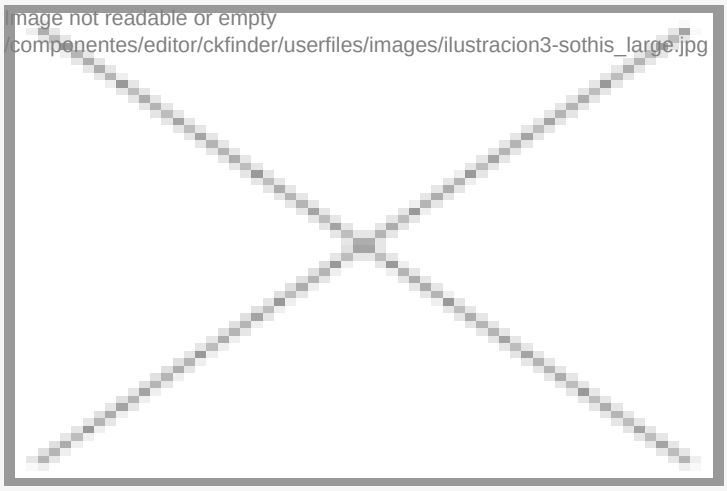

Ilustración 3: Email utilizado por el malware Koadic.

Otro malware que también ha sido polémico es AZORult, este troyano fue introducido en una versión descargable del mapa de la Universidad Johns Hopkins para equipos Windows que muestra como se está propagando el virus en el mundo (y que es ampliamente consultado).

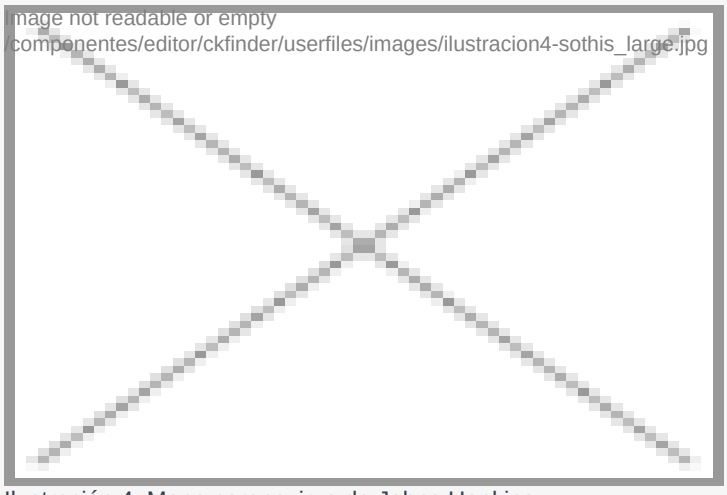

Ilustración 4: Mapa coronavirus de Johns Hopkins.

Por otro lado, las medidas de restricción de movilidad y la necesidad de tomar medidas preventivas para contener la propagación del virus ha provocado un aumento en la demanda de instalaciones de VPN (Redes privadas virtuales) para facilitar el teletrabajo a aquellos empleados de una organización susceptibles de utilizarlo.

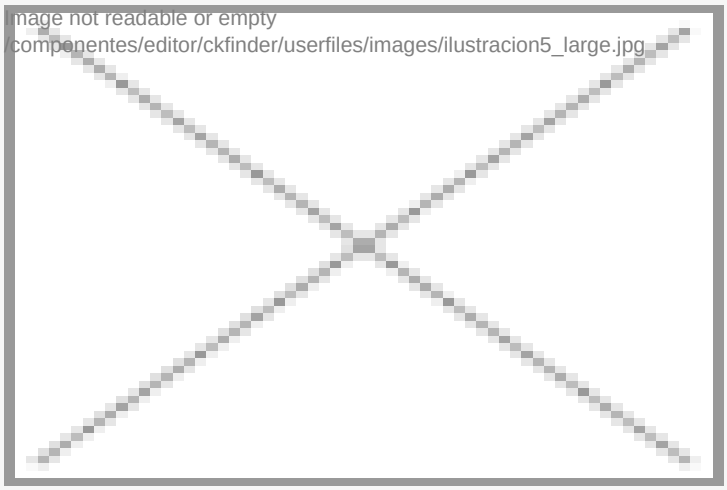

Ilustración 5: Comparación de nuevas conexiones VPN en 10h.

En algunos casos, la medida rápida de ofrecer teletrabajo en empresas donde no se estaba presente el servicio, está provocando fallos de seguridad por la falta de procedimientos y medidas de protección adecuados, ya lo dice dicho “las prisas nunca son buenas consejeras” y esto supondrá un incremento de ciberataques a los que las empresas necesitan responder para garantizar la seguridad de sus datos. Un vector que se está utilizando en este caso es el de ataques de ingeniería social, por medio de correo electrónico, en el cual los atacantes se hacen pasar por el departamento informático o de recursos humanos de la empresa para incitar a los empleados a que expongan sus credenciales corporativas en aplicaciones falsas para robarlas. De aquí que las empresas, a la vez que activan las conexiones VPN para sus usuarios, hagan entrega de un manual de buenas practicas para el uso de la misma y establezcan controles de seguridad que les permitan controlar quien, cuando y desde donde se conectan, de forma tal que puedan verificar que los usuarios conectados son los que dicen ser y lo hacen desde lugares y equipos perfectamente identificados y protegidos.

Consejos y buenas prácticas

Por todo lo comentado anteriormente, debemos de estar más atentos de lo que por lo general ya estamos y seguir estos prácticos consejos para no ser víctimas de un ciberataque:

1. No te fíes del nombre del emisor del mensaje

Cualquiera puede poner como remitente del mensaje el nombre que desee, por lo que siempre deberemos es contrastar que la dirección del email corresponda con la compañía que dice ser. Por ejemplo, nos llega un email de Amazon, pues la cuenta de correo debería de ser algo parecido a info@amazon.es y no info.amazon@yandex.ru. Para ello puedes pasar el cursor por encima de la dirección de correo que aparec y verás cuál es el origen del mismo (o puedes pisar botón derecho del ratón y ver la dirección de correo de origen del remitente)

2. No ejecutar archivos adjuntos o enlaces de remitentes que no sean de nuestra absoluta confianza

Si un desconocido o supuesta entidad conocida, pero no utiliza por ti o en tu empresa te pide que ejecutes un fichero o accedas a una supuesta aplicación para visualizar una supuesta factura, es muy probable que estés siendo víctima de un ataque de ingeniería social. Borra inmediatamente el correo y avisa al departamento de ciberseguridad de tú empresa.

3. No utilices la misma contraseña para más de una cuenta o servicio

Si llegas tarde a esta información y piensas que has podido ser víctima de un ataque de ingeniería social (phishing), cambia cuanto antes la contraseña de los servicios y habilita la autenticación de doble factor (2FA), si está disponible, que te ofrecerá una capa extra de seguridad, al requerir tu dispositivo móvil para autenticarte con éxito.

4. Habilitar el doble factor de autenticación (2FA)

Siempre y cuando la aplicación lo permita, nunca está de más habilitar esta medida de seguridad que te dará un nivel de protección adicional en nuestra cuenta.

Este servicio requiere hacer una doble verificación de identidad introduciendo un código que puede ser enviado a nuestro dispositivo móvil, o que se puede generar a través de aplicación especifica de autenticación, esto impediría a un atacante poder utilizar la cuenta comprometida, ya que, aun teniendo las credenciales correctas de acceso también necesitaría el código de verificación que será enviado a nuestro móvil.

5. Mantener actualizada la VPN y los dispositivos de trabajo

Actualizar las VPN, dispositivos de red y dispositivos que se utilizan de forma remota en entornos laborales con los últimos parches de software y configuraciones de seguridad.

Implementar MFA (Autenticación multifactor) en todas las conexiones VPN para aumentar la seguridad, además de utilizar contraseñas seguras y robustas.

6. Informar a los empleados sobre ataques de phishing

Alertar a nuestros empleados de un posible aumento de ataques de ingeniería social, ya sea vía email o telefónica, será un gran acierto para mantener la seguridad en nuestra empresa.

Y por supuesto, la realización de formaciones a los empleados de la organización sobre los peligros y funcionamiento de la ingeniería social es primordial para mantener una buena salud en cuanto a seguridad, recodemos que “el usuario, es el eslabón más débil”.

Con los anteriores consejos y siguiendo la guía de las medidas de seguridad para acceso remoto que nos proporciona el CCN-CERT, debería de ser suficiente para trabajar con seguridad desde casa.

Concienciación y sentido común

Nos reiteramos, no importa el tamaño de tú organización, la pandemia continúa creciendo y con ella, los ciberataques. Pero debemos permanecer tranquilos y actuar con cautela, nuestra preocupación y distracción serán las mejores aliadas de los ciberdelincuentes.

Fuente: redseguridad.com