



MEDINA & RIVERA
INGENIEROS ASOCIADOS S.A.S.

EL HACKEO O “RANSOMWARE” EN COLOMBIA

“Todo su trabajo y archivos personales fueron encriptados”. Con ese mensaje, pero en inglés (‘All your work and personal files were encrypted’) empezó el calvario de Carlos Ramírez (*), un colombiano de 25 años que fue víctima de una modalidad de crimen cibernético internacional con cada vez más impacto en Colombia: el ‘ransomware’. El término viene de las palabras en inglés ‘ransom’ (rescate) y ‘ware’ (programa) y no es otra cosa que un secuestro de los datos de su computador.

El asunto opera así: bien sea por la apertura de un documento adjunto que llegó en un correo electrónico, o bien por un archivo que al entrar a una página web se le pide descargar, la persona permite la entrada en su equipo de un programa malicioso que le encripta parte o la totalidad de los archivos de su máquina: documentos, videos, imágenes, etc. Acto seguido, la víctima recibe la notificación de que si quiere volver a tener acceso a esa información debe pagar una cantidad de dinero.

Ojo con dónde se mete:

A Óscar Méndez (*), un emprendedor, le pasó lo mismo. En su caso, buscaba el sitio web de una institución de educación superior de Colombia. Le dio clic al primer resultado arrojado por Google e ingresó a una página con una apariencia idéntica a la del portal real, pero que en realidad había sido montada por ciberdelincuentes.

Cuando entró a esa página, se le pidió instalar un complemento de Java para mejorar su navegación y él aceptó sin pensarlo. Horas después, se encontró con que todos sus archivos estaban bloqueados.

Este problema no solo afecta a los computadores, sino también a los dispositivos móviles, en particular a aquellos que operan con el sistema operativo Android. En un informe anual, la firma de seguridad informática Eset habla de un “auge del ‘ransomware’ para Android” y asegura que el número de casos creció un 50 por ciento durante el 2016.

En Colombia, el Centro Cibernético Policial empezó a registrar casos desde el 2015. Ese año hubo 13 afectados. Pero 12 meses después, el número se multiplicó por más de seis: 84 casos. Al cierre de febrero del 2017, ya iban 22, con lo que cabe esperar que el año termine con más de 100.

Si va a buscar un sitio oficial de un banco u otra entidad, no confíe ciegamente en los resultados arrojados por el motor de búsqueda. Cerciórese de que la dirección del portal visitado sea segura, es decir que empiece con https:// y no con el http:// tradicional.

Sospeche si le llega un correo con un asunto atemorizante o provocador. La amenaza de que le van a cerrar la cuenta bancaria, el video ‘hot’ de un famoso y la fotomulta son algunos ejemplos.

Programación ABRIL



| | |
|---------------------------------------|----|
| AVILES BLANCO JUAN FERNANDO | 3 |
| BONILLA CUBILLOS VICTOR HUGO | 5 |
| AMAURY CARRILLO GALVIS | 6 |
| ROGER ALEJANDRO CUSPOCA | 11 |
| VELEZ DIAZ JUAN GABRIEL | 11 |
| MIGUEL ANTONIO QUIROGA CORREA | 21 |
| YENCY LORENA DIAZ | 22 |
| QUITIAN DCAMPO CLAUDIA BIBIANA | 24 |
| DIA DE LA SECRETARIA | 26 |
| RAMIRO ERAZO ESTEBAN | 26 |
| QUILLERMO JOSE DE LA BARRERA CASTILLO | 26 |
| JAIMÉ ANIBAL NIÑO MENDIVELSON | 28 |
| DIA DEL NIÑO | 29 |

No abra ningún documento adjunto sobre el cual tenga el más mínimo porcentaje de duda.

No permita que sus hijos utilicen sus smartphones y más aún si allí tiene configurado el correo corporativo de la empresa.

Dude incluso de correos provenientes de amigos, que suelen replicar el ‘ransomware’ sin saberlo.

Fuente: EL TIEMPO 2 De Abril / 2017