CORREOS MALICIOSOS, TERROR HOY, MAÑANA Y… ¿SIEMPRE?

NOTI 279 – Agosto de 2018

Si tiene dudas sobre la autenticidad de un correo electrónico revise:

- Los nombres que figuran en el correo electrónico.
- Si el remitente está enviando el correo a nombre propio o de otra persona y qué coincidencias hay en los dominios de ambas direcciones electrónicas.
- Qué faltas de ortografía existen en el texto del correo.

Infecciones de Malware por país.

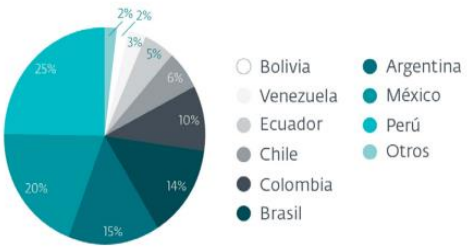
Fuente: ESET Security Report 2018

El uso de las tecnologías se ha vuelto esencial para el desarrollo de nuestras actividades personales y empresariales. Las herramientas tecnológicas han cambiado nuestra forma de relacionarnos con los demás, ha transformado la manera de hacer negocios, así como ha estructurado nuevas formas para realizar transacciones monetarias. Ha traído grandes beneficios representados tanto en tiempo como en dinero; sin embargo, debido a su masiva utilización, ha inspirado la creación de nuevas modalidades de delitos que han puesto en vilo la estabilidad económica y reputacional no solo de empresas sino de particulares.

La tendencia de crecimiento de los delitos informáticos es preocupante. Durante el 2017, de acuerdo a los datos revelados por ESET Security Report 2018, al menos 3 de cada 5 empresas de Latinoamérica sufrieron, mínimo, un incidente de infección con códigos maliciosos (45%). Existen muchas razones para que este tipo de eventos ocurran, entre las cuales están:

- Insuficientes o nulos sistemas de protección.
- Ausencia o escasa cultura de autocuidado en procesos informáticos.
- Limitado o cero conocimiento en el área.
- Bajas probabilidades de que los transgresores sean identificados y judicializados.

"…al menos tres de cada cinco empresas en la región sufrieron por lo menos un incidente de seguridad, estando en el top la infección con códigos maliciosos (45%)". ESET



Detecciones de Filecoder en países de LATAM durante 2017

Fuente: ESET Security Report 2018

Lo anterior no significa que empresas o personas con amplios sistemas de protección, educación y cultura informática estén exentos de ser víctimas de este tipo de eventos, pero sí les dificulta la labor a los delincuentes.

Son varias las recomendaciones que todos los días se publican para evitar la contaminación de nuestros sistemas informáticos con los Malware, inclusive en nuestro NOTI 257 del 8 de noviembre de 2016 hicimos algunas sugerencias, pero aun así sigue pasando y es muy común que sigamos cayendo con el método preferido por los delincuentes: correos electrónicos con contenido malicioso.

Estos defraudadores envían correos masivos que, aparentemente, llegan de remitentes conocidos, contactos profesionales o de entidades públicas con enlaces o archivos adjuntos que pueden ser: texto, imágenes o programas; los cuales, una vez ejecutados, infectan los equipos y luego toda la red, con resultados que pueden ir desde daños en máquinas o programas, pasando por suplantación de identidad, hasta llegar al secuestro de información.

Si tiene dudas sobre la autenticidad de un correo electrónico revise:

- Los nombres que figuran en el correo electrónico. En los casos de comunicaciones oficiales o empresariales, generalmente, el nombre de la entidad no corresponde con el real, aunque a simple vista no nos percatemos de ello. Es así como el Ministerio de Transporte se puede convertir en Ministerio de Tránsito.

- Si el remitente está enviando el correo a nombre propio o de otra persona y qué coincidencias hay en los dominios de ambas direcciones electrónicas.

- Qué faltas de ortografía existen en el texto del correo. Puede ser que existan errores ortográficos en comunicados legítimos, pero hay cosas que deben llamar la atención como la escritura de nombres propios en minúscula, por ejemplo, en vez de Medellín veremos medellin.

- Si estaba esperando algún mensaje del remitente.

Lo mencionado anteriormente solo hace parte de un gran número de detalles que se pueden observar en un correo malicioso. Cabe recordar que siempre puede comunicarse telefónicamente con la persona o entidad que envió el correo para comprobar su autenticidad.

martes 17/07/2018 10:17 a. m.
contactosvison@mail-zg367.getresponse.com en nombre de Ministerio De Transito <ministerio@transporte-gov.co>
Notificacion De Foto Comparendo Nº 699403

17 De julio Del 2018

ACTA DE INFRACCIÓN DE TRÁNSITO

Orden de comparendo Nº 699403

SEÑOR CONDUCTOR

Se notifica a usted que presenta un comparendo por foto multa, valor de la sanción $ 355.700 (trescientos cincuenta y cinco mil setecientos pesos)

COMPARENDO C48; Ley 1212 del 25 de marzo del 2009:Conducir un vehículo a velocidad superior a la máxima permitida

se le anexa a descargar archivos adjuntos en el siguiente enlace donde encontrara fotos hora y lugar donde se origino su comparendo

DESCARGUE AQUÍ SU COMPARENDO

• EVIDENCIAS: FOTOS, LUGAR Y FECHA DE LA INFRACCIÓN

NOMBRE DEL "REMITENTE", carrera 65 numero 32 10, bogota, cundinarmarca 110111, Colombia
Usted puede darse de baja o cambiar sus datos de contacto en cualquier momento

Si usted abrió algún archivo, siguió un enlace o ejecutó un programa de un correo electrónico sospechoso, notifique de inmediato al área de sistemas, saque su equipo de la red y no lo apague. El encargado de T.I. realizará el procedimiento correspondiente para conservar la integridad de los sistemas de información y del Hardware. En caso que sea su equipo personal, desconecte el Internet y póngalo en cuarentena o busque ayuda de un técnico.

asr@asr.com.co

Carrera 43B N° 16-41
Medellín, Colombia
+57 4 311 11 55
asr@asr.com.co
www.asr.com.co