Los crímenes cibernéticos que se propagan con el coronavirus

Los criminales en Internet se han aprovechado de la preocupación de los usuarios por la propagación del coronavirus para hacer de las suyas.

Son varios los correos que circulan en Internet que pretenden alertar a la comunidad sobre riesgos de la enfermedad, bajo el nombre de alguna entidad gubernamental. Sin embargo, esta información puede ser una herramienta utilizada por cibercriminales para robar la información de quienes acceden a los archivos adjuntos enviados.

En los correos se usa como fachada la enfermedad, que hasta ahora se ha cobrado la vida de más de 3.000 personas e infectado a cerca de 90.000 individuos en todo el mundo, para enviar archivos maliciosos camuflados en PDF, MP4 y dock y que usan para acceder a la información personal de quienes caen en la trampa.

Una vez los cibercriminales acceden a la información personal de los usuarios pueden suplantar su identidad y entrar a sus cuentas bancarias para robar el dinero.

Según Kaspersky, una firma especializada en el área de ciberseguridad, su sistema de detección encontró archivos que contenían una variedad de amenazas, desde troyanos hasta gusanos que son capaces de destruir, bloquear, modificar o copiar datos, así como interferir con el funcionamiento de las computadoras o redes de cómputo.

Los casos más sonados giran en torno a la Organización Mundial de la Salud (OMS). Los criminales usan el nombre de la entidad con reconocimiento internacional para engañar a la mayor cantidad de víctimas posibles.

Por medio de correos electrónicos, enviados supuestamente por la institución, se les advierte a las personas de la gravedad e impacto de la nueva enfermedad y se les pide abrir una serie de archivos adjuntos que contienen más información acerca del virus.
“Acceda al documento adjunto para conocer las medidas de seguridad contra la propagación del coronavirus. Dé clic en el botón debajo para descargar los síntomas comunes que incluyen fiebre, tos y problemas al respirar”, reza en uno de los correos

difundidos en línea.

En el mensaje se adjunta un enlace que no cuenta con los protocolos de seguridad adecuados ya que el hipervínculo tiene la dirección http en vez de https, además de la detección de errores de ortografía y redacción que indican una conducta sospechosa.
Cuando los usuarios interesados en la información de prevención del coronavirus ingresan, la página les pide escribir un usuario y una contraseña, al hacerlo le dejan su información expuesta a lo criminales cibernéticos.

Según Roberto Martínez, analista sénior de seguridad de Kaspersky, los medios más usados por estos delincuentes son las páginas web y el correo electrónico; sin embargo, también lo hacen a través de las redes sociales.

“Por medio de la autenticidad de las páginas y las notas sensacionalistas, los criminales buscan clics de los usuarios y de esa manera direccionarlos a un sitio donde pueden infectar sus equipos y cometer el delito”.

Otro caso de delincuencia que se vale del nombre de la OMS es el de un esquema de supuestos representantes de la entidad que piden donaciones para ayudar a los afectados por el coronavirus. Aunque los criminales no roban información ni insertan malware en los dispositivos, sí se aprovechan de la empatía de la gente con los afectados para lograr transacciones de dinero.

Maximiliano Cantis, especialistas en seguridad informática de la firma Safetica, asegura que “los criminales cibernéticos no solo usan la enfermedad para causar daños individualmente, sino también lo hacen de forma colectiva”, por ejemplo, en Ucrania, la semana pasada se divulgó un correo que afirmaba que en el país había cinco personas contagiadas por coronavirus, lo que provocó fuertes protestas que llevaron al cierre de carreteras y destrucción de buses en los que se desplazarían personas evacuadas de Wuhan, epicentro del virus.

¿Cómo no caer?

Roberto Martínez recomienda a quienes reciban este tipo de correos o decidan buscar información en la web sobre temáticas relacionadas con el nuevo coronavirus u otras coyunturas evitar acceder a enlaces sospechosos que prometen contenido exclusivo.
Cuando la información en internet o los e-mails tengan información “demasiado buena para ser cierta o parezca ser demasiado sensacionalista, mejor consultar las fuentes oficiales

para obtener información confiable y legítima”.

Es importante asumir que siempre se está expuesto a caer en este tipo de engaños, por lo que es necesario revisar las extensiones de los archivos que se quieren descargar (documentos y archivos de video no corresponden al formato .exe o .lnk).
Además de utilizar una solución de seguridad confiable como un antivirus que monitoreé los dispositivos para identificar cualquier amenaza.

“Acceda al documento adjunto para conocer las medidas de seguridad contra la propagación del coronavirus. Da clic en el botón debajo para descargar. Los síntomas comunes incluyen fiebre, tos, y problemas al respirar”, reza en el correo.

Con información de El Tiempo