Aumentan las campañas de malware que aprovechan el miedo causado por el COVID-19

ESET Latinoamérica quiere advertir de un gran **incremento de campañas maliciosas** en las que los cibercriminales intentan aprovecharse de la situación del coronavirus para comprometer a los usuarios.

En estos últimos días también **se han registrado ciberataques** a organismos o instituciones de salud que tienen un rol significativo en la lucha para evitar el avance de la pandemia, como el ciberataque al Hospital Universitario de Brno, en República Checa, en el cual funciona uno de los 18 centros de pruebas sobre el coronavirus en ese país, o el ataque de DDoS al Departamento de Salud Estados Unidos.

Desde ESET España alertaron esta semana sobre un **correo de phishing**, en un correcto español, que hace **alusión a la preparación de una vacuna casera para evitar la enfermedad.** El falso correo incluye un adjunto que contiene la supuesta lista de elementos necesarios para preparar la falsa vacuna, que esconde un troyano. Asimismo, ESET también detectó una versión igual en un correo en portugués.

Hace unos meses ESET publicó **un análisis sobre Casbaneiro**, un troyano bancario que afecta principalmente a países como México y Brasil y se detectó actividad reciente con una campaña en la que los operadores de este **troyano están aprovechando COVID-19 para infectar a los usuarios.**

A su vez, se descubrió un **ransomware oculto en una falsa aplicación para el monitoreo del coronavirus.** Denominado CovidLock, esta aplicación, ofrece un mapa de calor con datos estadísticos sobre el avance del virus en el mundo. Sin embargo, tras analizar este el dominio sospechoso, se identificó que la app ocultaba un ransomware para Android que bloquea a la víctima el acceso al dispositivo, al cambiar la contraseña que utiliza el usuario y asi secuestrando el teléfono. Luego despliega a la víctima un mensaje en el cual amenaza con robar y enviar la información que contiene el dispositivo a cambio del pago de $250. Según el **investigador de ESET, Lukas Stefanko**, quien analizó la amenaza, quienes hayan sido víctima de este ransomware podrán desactivarlo usando el código de desbloqueo ”4865083501”.

“A la preocupación que ha generado el avance de COVID-19, los usuarios y empresas deben estar atentos a estos engaños que crecen día a día, sobre todo en momentos como los actuales donde muchas empresas han tomado la medida de que los empleados trabajen de manera remota para permanecer en sus casas. Como siempre, desde ESET apostamos a la educación y concientización, tomando medidas básicas como contar con una solución de seguridad confiable tanto en equipos de escritorio como en dispositivos móviles, actualizar los sistemas y evitar dar clic sin a cualquier enlace sin antes chequear que sea seguro, De esta manera podemos disfrutar de Internet de manera segura”, aconseja **Camilo Gutiérrez, Jefe del Laboratorio de Investigación de ESET**

Latinoamérica.