Coronavirus:

cómo los piratas informáticos están usando el miedo a la enfermedad covid-19 para difundir virus informáticos

Coronavirus:

cómo los piratas informáticos están usando el miedo a la enfermedad covid-19 para difundir virus informáticos

Todo comienza con un clic inocente.
A medida que el nuevo coronavirus surgido en China se propaga por todo el mundo, los piratas informáticos utilizan el miedo y la confusión para expandir virus informáticos de maneras cada vez más sofisticadas.

SE HA ESTADO RASTREANDO ALGUNAS DE LAS ESTAFAS DE PHISHING POR CORREO ELECTRÓNICO REPORTADAS POR LAS ORGANIZACIONES DE CIBERSEGURIDAD DESDE QUE EL BROTE DEL NUEVO CORONAVIRUS SALTÓ A LAS PORTADAS.

SE HAN DETECTADO CIENTOS DE DIFERENTES CAMPAÑAS CRIMINALES QUE HAN ENVIADO MILLONES DE CORREOS ELECTRÓNICOS FALSOS.

El fraude de la extorsión a la novia de tu amigo cuya verdadera víctima puedes acabar siendo tú
No es nuevo que las campañas de phishing echen mano de la actualidad, pero los expertos en seguridad de la información dicen que el aumento en los ataques relacionados con el covid-19, la enfermedad que provoca el nuevo coronavirus, es el peor visto en años.

Los ciberdelincuentes están usando el inglés, francés, italiano, japonés y turco para dirigirse a las posibles víctimas, tanto individuos como industrias que incluyen la del transporte, la atención médica, las aseguradores, los hoteles, la restauración y la manufactura.
Es imposible decir cuál es la verdadera escala de la epidemia de correos electrónicos, pero aquí tienes algunos de los más convincentes y cómo detectarlos.

"HAZ CLIC AQUÍ PARA LA CURA DEL CORONAVIRUS"

Es un mensaje de un médico misterioso que afirma tener un documento con detalles sobre una vacuna contra el coronavirus que está siendo encubiertos por los gobiernos de China y Reino Unido.

los destinatarios curiosos que hacen clic en el documento son llevados a lo que parece una página normal y confiable de Docusign, pero en realidad es una web creada por los propios delincuentes para obtener sus datos de inicio de sesión.

Una vez que obtienen el nombre de usuario y la contraseña, se apoderan de sus documentos, además de que conseguir acceso a cualquier otro sitio que use el mismo correo electrónico y contraseña. Los correos electrónicos se envían en lotes de 200.000 a la vez.

La mejor manera de ver dónde te llevará un enlace es pasar el cursor sobre él, donde aparecerá la verdadera etiqueta URL. Si parece sospechosa, no hagas clic.

"OMS: este consejo puede salvarte"

» Los piratas informáticos se han hecho pasar por la Organización Mundial de la Salud (OMS) desde los primeros días del brote, una estrategia particularmente censurable.

Fuente de información:
https://www.bbc.com/

Los analistas dicen que las víctimas que descargan el archivo que trae adjunto no reciben ningún consejo útil y, en cambio, sus computadoras quedan infectadas por un malware llamado AgentTesla Keylogger.

Una vez instalado, este malware registrará todas las pulsaciones de teclas y lo enviará a los atacantes, una táctica que puede dar acceso por internet a cuentas bancarias y financieras.

Para evitar esta estafa, ignora correos electrónicos que supuestamente provienen de la OMS, ya que probablemente sean falsos y, en su lugar, visita el sitio web oficial de la institución o sus canales de redes sociales para ver sus últimos consejos.
“Ahora el virus está en el aire

Esta campaña de phishing no solo es llamativa, sino que induce al miedo.
El asunto dice "covid-19: ahora en el aire, transmisión comunitaria incrementada" y también está diseñado para parecerse a un correo electrónico del Centro para el Control y la Prevención de Enfermedades (CDC, por sus siglas en inglés), la agencia estadounidense encargada del área sanitaria, con una dirección falsa que es muy convincente.

Los analistas dicen que el enlace dirige a las víctimas a una página de inicio de sesión falsa de Microsoft donde se les anima a ingresar un correo electrónico y una contraseña. Una vez que lo hacen, son redirigidas a la página real de consejos de los CDC, lo que hace que parezca aún más legítimo.
Por supuesto, para cuando llegas ahí los defraudadores ya tienen lo que necesitan de tu cuenta de correo electrónico para saquearla cuando lo deseen.

Tú puedes evitar la suplantación de identidad con un servicio VPN de acceso remoto, contácta a nuestros especialistas.