Según un informe publicado por Check Point Research, hackers están explotando el brote de COVID-19 para propagar sus propias infecciones, incluido el registro de dominios maliciosos relacionados con coronavirus y la venta de malware con descuento en la deep web.

> *«Las ofertas especiales de diferentes piratas informáticos que promocionan sus productos – generalmente malware malicioso o herramientas de explotación – se venden por medio de la red oscura bajo ofertas especiales con 'COVID19' o 'coronavirus', como códigos de descuento, dirigidos a los posibles atacantes cibernéticos»*, dicen los investigadores.

Este informe se produjo luego de un aumento en la cantidad de dominios maliciosos relacionados con el coronavirus que se han registrado desde inicios de enero.

> *«Sólo en las últimas tres semanas (desde finales de febrero de 2020), hemos notado un gran aumento en el número de dominios registrados: el número promedio de dominios nuevos es casi 10 veces más que el número promedio encontrado en semanas anteriores. Se descubrió que el 0.8 por ciento de estos dominios eran maliciosos (93 sitios web), y otro 19 por ciento era sospechoso (más de 2200 sitios web)»*, agregaron.

Algunas de las herramientas disponibles para la compra a un precio con descuento incluyen *«Evitar WinDefender»* y *«Compilar para evitar la seguridad de correo electrónico y Chrome».*

Otro grupo de piratería bajo el nombre de *«SSHacker»*, ofrece el servicio de piratería en la cuenta de Facebook con un descuento del 15% con el código de promoción *«COVID-19».*

Además, un vendedor conocido como *«True Mac»,* está vendiendo un modelo de MacBook Air 2019 por solo 390 dólares, como una *«oferta especial de corona».* Obviamente se trata de una estafa.

Ataques cibernéticos relacionados con el coronavirus

Últimamente de han disparado los ataques cibernéticos contra hospitales y centros de pruebas, además de campañas de phishing que distribuyen malware como AZORult, Emotet, Nanocore RAT y TrickBot por medio de enlaces maliciosos y archivos adjuntos, que posteriormente ejecutan ataques de malware y ransomware que tienen como objetivo obtener beneficios por la preocupación mundial por la salud.

APT36, un grupo de piratería patrocinado por el estado de Pakistán que se dirige a la defensa, las embajadas y el gobierno de la India, se encontró ejecutando una campaña de phishing mediante cebos de documentos con temática de coronavirus que se hicieron pasar por avisos de salud para desplegar la Herramienta Crimson Remote Administration Tool (RAT) en sistemas de destino.

Por otro lado, investigadores de la compañía de seguridad IssueMakersLab, descubrieron una campaña de malware lanzada por hackers norcoreanos que utilizaba documentos que detallaban la respuesta de Corea del Sur a la epidemia de COVID-19 como un señuelo para eliminar el malware BabyShark.

Una campaña de malspam con temas sobre COVID-19, que tiene como objetivos industrias de la fabricación, industrial, finanzas, transporte, farmacéutica y cosmética, utiliza documentos de Microsoft Word para aprovechar errores de Microsoft Office en el Editor de Ecuaciones, para instalar AZORult malware. Este malware también ha sido propagado mediante una versión fraudulenta del mapa de coronavirus de Johns Hopkins.

También se descubrió que una aplicación para Android falsa de seguimiento de coronavirus en tiempo real, llamada *«COVID19 Tracker»,* abusó de los permisos de los usuarios de los usuarios para cambiar la contraseña de la pantalla de bloqueo del teléfono e instalar el

ransomware CovidLock a cambio de un rescate de 100 dólares en Bitcoin.

Otro ataque de phishing, descubierto por Abnormal Security, apuntó a estudiantes y personal universitario con correos electrónicos falsos en un intento por robar sus credenciales de Office 365 al redirigir a las víctias desprevenidas a una página de inicio de sesión falsa de Office 365.

Investigadores de F-Secure observaron una nueva campaña de correo no deseado que tiene como objetivo capitalizar la escasez generalizada de máscaras para engañar a los destinatarios para que paguen máscaras, para que al final no envíen el producto.