Microsoft anunció la habilitación de la búsqueda guiada de amenazas con temática de COVID utilizando las computadoras portátiles Azure Sentinel, con la finalidad de detectar a la gran cantidad de ataques cibernéticos relacionados con dicha temática para proteger a los usuarios.

Según la compañía, los clientes de Microsoft Threar Protection (MTP), ya se encuentran protegidos contra las amenazas identificadas por estos indicadores en los puntos finales con Microsoft Defender Advanced Threat Protection (ATP) y correo electrónico con Office 365 ATP.

La compañía también mencionó que ha publicado información esencial sobre las técnicas de los atacantes, para que los usuarios que aún no utilizan MTP, sepan como detectar este tipo de ataques cibernéticos.

> *«Además, estamos publicando estos indicadores para aquellos que no están protegidos por Microsoft Threat Protection para crear conciencia sobre el cambio en las técnicas de los atacantes, cómo detectarlos y cómo habilitar su propia caza personalizada. Estos indicadores ahora están disponibles de dos maneras. Están disponibles en Azure Sentinel GitHub y a través de la API de seguridad de Microsoft Graph . Para los clientes empresariales que usan MISP para almacenar y compartir inteligencia sobre amenazas, estos indicadores se pueden consumir fácilmente a través de un feed MISP*«, escribió la compañía en su blog.

Microsoft asegura que su feed de inteligencia de amenazas específico de COVID, representa un comienzo para poder compartir algunos de los IOC relacionados con COVID de Microsoft.

En lanzamiento de hoy por parte de Microsoft, cuenta con indicadores de hash de archivos relacionados con adjuntos basados en correo electrónico identificados como maliciosos y que intentan engañar a los usuarios con COVID-19 o señuelos temáticos de coronavirus.

> *«Microsoft Threat Protection brinda protección para las amenazas asociadas con*

> *estos indicadores. Los ataques con estos indicadores temáticos de Covid-19 están bloqueados porOficina 365 ATP y Microsoft Defender ATP. Si bien los clientes de MTP ya están protegidos, también pueden usar estos indicadores para escenarios de caza adicionales utilizando las capacidades de caza avanzada de MTP»*, dice la compañía.