ravenloop
Intelligence evolved

Malware vs Enfermedad

Clara Martínez

NEWS
CLICKCIBER

¿Puede ayudarnos la ciber inteligencia a prevenir futuras pandemias?

El software malicioso (o **malware** en término anglosajón), y las enfermedades infecciosas como el sars-cov-2 comúnmente conocido como covid-19, son similares en varios aspectos. Habitualmente nos referimos al software malicioso en términos de "virus" y "gusanos", en parte por el nivel de similitud en el patrón de **ataque**, pero también porque el contagio de cualquiera de los tipos puede amenazar a toda una comunidad. La globalización de la economía facilitada por las **TIC**, ha incrementado las relaciones comerciales, viajes y transporte de mercancías por todo el mundo por lo que no es la primera vez que se han producido brotes a través de las personas, como el MERS-CoV en 2012 en Oriente Medio *(OMS 11 de marzo del 2019)* o el del ébola en África occidental *(Kara Rogers, 2014*). Siguiendo con la analogía de propagación de estos virus a los individuos, el malware que abarca una amplia tipología, desde **Conficker** y **Zeus** hasta Emotet- se ha extendido por todo el medio digital durante los últimos años. Al igual que en las enfermedades, estas amenazas tienen una serie de características comunes que conviene identificar en la medida que pueden ayudarnos a reforzar la **seguridad** de los entornos digitales de las empresas.

En primer lugar, en ambos casos pueden llegar a ser muy contagiosas y estar muy extendidas, no obstante, la transmisibilidad varía: no todos los ataques cibernéticos se transmiten o tienen la intención de propagarse más allá de un computador específico. Sin embargo, el potencial de **propagación** significa que la **amenaza** para cualquier individuo o computadora depende en parte de la salud de la población o red en general. Esta interdependencia también indica que asegurar cualquier tipo de sistema mediante **inteligencia** o vigilancia depende en parte de la cooperación local, nacional e internacional.

En segundo lugar, tanto el **malware** como las enfermedades tienen efectos no cinéticos que pueden ser difíciles de detectar. Esta dificultad complica la vigilancia y la atribución de fuentes porque los síntomas pueden retrasarse, ocultarse o ser inespecíficos, dejando a las víctimas y los vectores inconscientes. Por tanto, la detección, el diagnóstico y el tratamiento requieren de conocimientos específicos en el área de seguridad y el uso de herramientas especializadas”

*“Es posible combatir las amenazas biológicas desde una perspectiva **tecnológica**”*

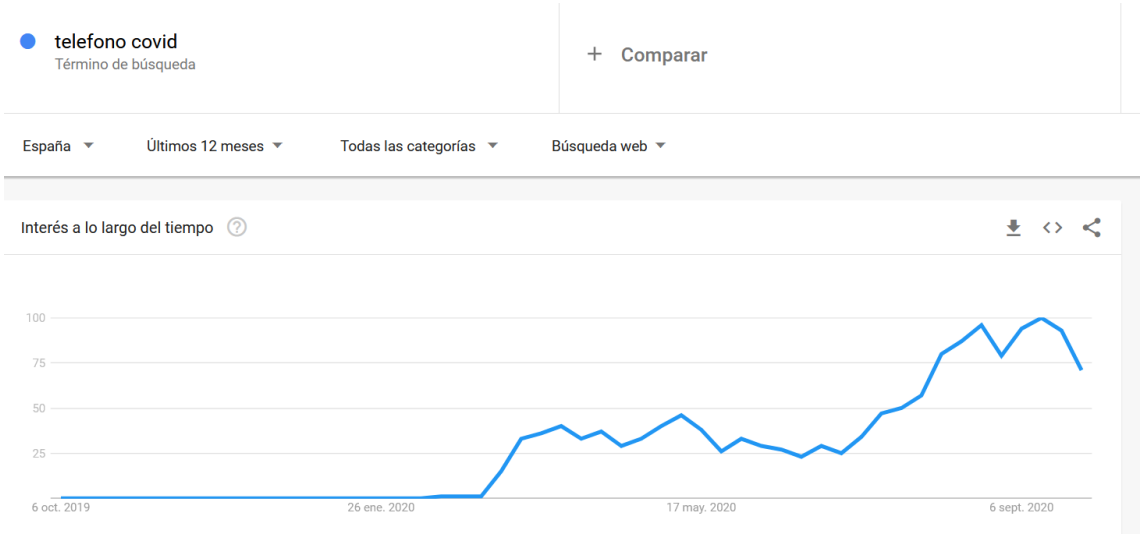
En definitiva, los requisitos funcionales para la **vigilancia** y la **inteligencia** necesaria para defendernos de estas amenazas son extremadamente importantes en ambos entornos, y la **tecnología** ya cuenta con soluciones **ciber inteligentes,** preparadas para combatir las amenazas biológicas que ponen en riesgo nuestras vidas cada día.

¿Pero, cómo podemos anticiparnos?

Actualmente, los analistas de datos trabajan con múltiples **herramientas** para identificar patrones y tendencias en múltiples plataformas y aplicaciones (*ver Epidemic intelligence tools and information resources).* Tales como **Google Trends**, que identifica los términos de búsqueda más populares en Google, y permite filtrar por fecha, país, ciudad y hasta por palabra o grupo de palabras clave. Estas funciones ya han sido aplicadas en diversos estudios como método de predicción de brotes de distintas enfermedades infecciosas, como la fiebre del dengue, la conjuntivitis la malaria o la gripe (Madhur Verma Octubre 2018), (Jeremy Ginsberg, Febrero 2009),(Michael S Deiner Septiembre 2019).

Los resultados de estos estudios destacan que, tras realizar ciertas consultas para obtener las búsquedas realizadas por los usuarios y el posterior análisis de éstas, se podrían haber detectado los brotes entre 2 y 3 semanas antes de que se produjeran.

Para convertir estas búsquedas en inteligencia de datos, es necesario que la información sea concisa, y en el caso del **covid-19** al tratarse de un virus nuevo, los síntomas de la enfermedad son fácilmente confundibles con los de otras enfermedades como la gripe. No obstante, el almacenamiento de cierta información clave es relevante para la detección de un nuevo brote, como por ejemplo “teléfono covid”, frecuentemente utilizada por los ciudadanos en el caso de sospecha de síntomas de covid19.



Ejemplo de búsqueda en Google Trends

El Gobierno de España ha puesto a disposición de las Comunidades Autónomas la aplicación “**Radar Covid**”, que permite detectar los casos positivos en el momento en el que el usuario sube los resultados de su diagnóstico. El uso de los datos recopilados por esta aplicación y otras fuentes como **Google Trends**, podrían ser clave para ayudar a interrumpir las cadenas de transmisión del virus.

Según el Informe Global Digital de 2019, el 57% de la población mundial tiene acceso a Internet y se prevé que en los próximos diez años alcance a la totalidad. En España, según datos de INE, 2019, la cifra de internautas entre 16 y 74 años alcanza al 90,7%, si bien no todas las personas

tienen las habilidades técnicas necesarias lo que aumenta la desconfianza o el escepticismo en el uso de aplicaciones como Radar Covid.

Por otro lado, con la llegada del **5G**, será posible ofrecer conectividad a un mayor núcleo de personas, con mayor velocidad y menor latencia.

La ciberseguridad es importante para la salud pública

La **ciberseguridad** juega a su vez un papel importante en la gestión de la salud pública. La confidencialidad, integridad y disponibilidad de la **información** en el ámbito clínico son vitales para salvaguardar la integridad y la vida de los pacientes, que cada vez más son susceptibles de **ciberataques**, lo que representa un desafío para el desarrollo de potentes soluciones de seguridad.

Sin embargo, no se trata únicamente de la protección de la información, sino de lo que hacemos con esa información, convirtiéndola en **inteligencia** que nos permita prepararnos frente a futuras amenazas tanto tecnológicas como biológicas.

Los profesionales de la **ciberseguridad** no nos cansamos de recomendar a las empresas que apuesten por reforzar sus entornos digitales, especialmente a aquellas que traten con datos sensibles como son los relacionados con los pacientes en un entorno sanitario, con el objetivo no solo de prevenir sino de **predecir** posibles ataques en el futuro.

Referencias

1. Middle East respiratory syndrome coronavirus (Mers-CoV). (11 de marzo del 2019). https://www.who.int/en/news-room/fact-sheets/detail/middle-east-respiratory-syndrome-coronavirus-(mers-cov)
2. Ebola Outbreak of 2014-2016. Kara Rogers. https://www.britannica.com/topic/Ebola-outbreak-of-2014
3. Epidemic intelligence tools and information resources https://www.ecdc.europa.eu/en/threats-and-outbreaks/epidemic-intelligence
4. Google Search Trends Predicting Disease Outbreaks: An Analysis from India. Madhur Verma, Kamal Kishore, Mukesh Kumar. (Octubre 2018) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6230529/
5. Detecting influenza epidemics using search engine query data. Jeremy Ginsberg, Matthew H. Mohebbi, Rajan. S Patel (Febrero 2009) http://static.googleusercontent.com/media/research.google.com/en/us/archive/papers/detecting-influenza-epidemics.pdf
6. Google Searches and Detection of Conjunctivitis Epidemics Worldwide. Michael S Deiner, Stephen D MCLeod, Jessica Wong. (Septiembre 2019) https://pubmed.ncbi.nlm.nih.gov/30981915/

Avd. Fuente Nueva 12A

28703, SS.RR. Madrid, España

Telf. 912 532 315

Email: sales@ravenloop.io