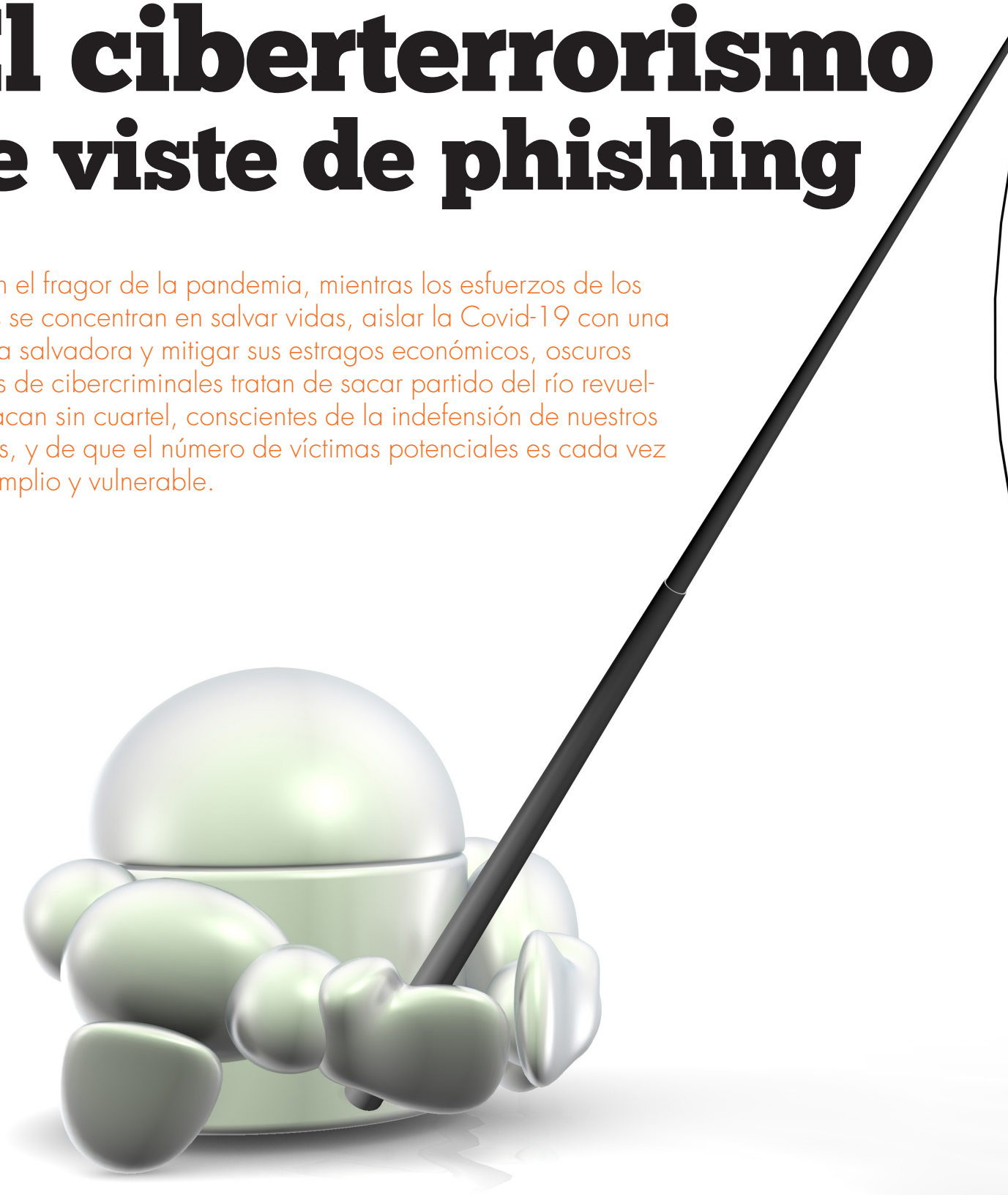
Texto
R. Contreras

ARRECIAN LOS ATAQUES QUE UTILIZAN COVID-19 COMO SEÑUELO

El ciberterrorismo se viste de phishing

<< En el fragor de la pandemia, mientras los esfuerzos de los países se concentran en salvar vidas, aislar la Covid-19 con una vacuna salvadora y mitigar sus estragos económicos, oscuros grupos de cibercriminales tratan de sacar partido del río revuelto. Atacan sin cuartel, conscientes de la indefensión de nuestros flancos, y de que el número de víctimas potenciales es cada vez más amplio y vulnerable.



Podría equipararse esta situación al terrorismo yihadista, por su dispersión y ejecución espontánea. Eugene Kaspersky, desarrollador ruso creador de la empresa homónima, ha sido tajante al respecto: "Cualquier ataque a un hospital en este momento puede ser visto como equivalente a un ataque terrorista". Su mensaje, a la vez que realista, no resulta tranquilizador, dado que las medidas de distanciamiento social no impactarán en la ciberseguridad. "Es muy probable que los ciberdelincuentes permanezcan activos. Están acostumbrados a trabajar desde casa y sus circunstancias no han cambiado drásticamente. Seguirán tratando de atacar a las empresas y a las personas y es nuestra obligación seguir trabajando duro y defender a nuestros clientes", advierte.

En cuanto al panorama general de amenazas, en los últimos meses se ha observado un aumento de los ataques tanto oportunistas como selectivos, y de las campañas de 'spear phishing', en particular, que suponen un importante reto ya que se dirigen a usuarios con consejos falsos relacionados con el coronavirus. Kaspersky ha observado un crecimiento del 43% en este tipo de ataques entre enero y marzo de 2020.

El entorno sanitario español, y en especial los hospitales, no escapa a los ciberataques. En los últimos dos meses se ha detectado un incremento de actividad cibernética maliciosa, utilizando Covid-19 como vector de ataque. Según datos recientes de Trend Micro, España se sitúa en el noveno puesto de los principales países que alojan URL maliciosas relacionadas con el virus, utilizadas para campañas de phishing o con fines de ciberdelincuencia. Es por ello que cabe extremar la precaución frente a las ciberamenazas que utilizan como señuelo la pandemia mundial. Desde enero se han realizado principalmente campañas de phishing relacionadas con la Covid-19 (un 54,70%), seguido de malware (un 34,30%), campañas de scam (7,50%) y otros vectores (1,50%).

¿Por qué atacar al sector sanitario?

GMV distingue cuatro factores determinantes que explican esta efervescencia del malware en la sanidad. En primer lugar, el coste medio de una brecha de datos en el sector sanitario se cotiza a 408 dólares por historial médico, frente a los 225 euros que se paga en el resto de las industrias. En la Deep Web se puede adquirir el historial clínico de los pacientes por 80 euros. En segundo lugar, la tecnología de los hospitales, heterogénea y con sistemas antiguos de más de 20 años, con redes mal segmentadas… conforma un blanco apetecible por las bajas dificultades que plantean a los cibercriminales. El robo de propiedad intelectual es otro motivo de peso, como explica el estudio de GMV: "La investigación médica es costosa y algunos grupos de amenazas persistentes avanzadas (APT), especializados en el robo de propiedad intelectual, atacan a institutos de investigación médica y empresas farmacéuticas que habitualmente llevan a cabo investigaciones innovadoras para hacerse con sus desarrollos". De hecho, la caza de la vacuna es una obsesión del 'lado oscuro', y así lo ha advertido el FBI. El cuarto vector es, aunque llueva sobre mojado, el factor humano. Los ciberdelincuentes hicieron uso del ransomware Netwalker para aprovechar las defensas bajas de los facultativos centrados en atajar la enfermedad, asediados por una incesante lluvia de contagios.

Pero el peligro no está solo en troyanos perniciosos como Emotet o Trickbot, o en los ransomware Netwalker o Ruyk, no hay que perder de vista a los ataques de denegación de servicio DDoS: "Durante la cuarentena, proliferó este tipo de ataques que saturan los sistemas informáticos de hospitales de Francia y República Checa o el portal web del Gobierno australiano", colapsando sus sistemas informáticos.

El hecho de que los ataques alcancen a todo el planeta no puede servir de consuelo. Proofpoint asegura que solo algún ministerio en España y ocho comunidades autónomas contemplan medidas de protección en sus servidores de correo electrónico ante posibles suplantaciones de identidad. La misma

"Hemos empezado a observar una mayor preocupación por parte de nuestros clientes en ciberseguridad y todo hace prever que entre finales de 2020 y 2021 aumente la inversión TI"

"España cuenta con una legislación moderna, con una fiscalía especializada y unas capacidades a nivel policial que se han adaptado a los tiempos y han evolucionado"

fuente señala que el 83% de las empresas del Ibex está en riesgo de que los ciberdelincuentes envíen correos electrónicos falsos a usuarios en su nombre.

¿Estamos en guerra?

En este estado de cosas, recurrir a los expertos de la Guardia Civil puede ayudar a aclarar este panorama tan turbio. ¿Está España preparada para aguantar el arreón ciberterrorista? José Durán, comandante de la Guardia Civil, perteneciente a la Unidad de Coordinación de Ciberseguridad, está convencido de nuestra posición. "España es uno de los países del mundo con mejores capacidades en cuanto a ciberseguridad, séptimo en el último GCI (Global Cybersecurity Index), ranking mundial elaborado por la Unión Internacional de Telecomunicaciones". Pero no basta con eso, "contamos con una Estrategia Nacional de Ciberseguridad y unas estructuras modernas y adaptadas a los tiempos actuales, con organismos especializados como Incibe y el CCN, con un sector privado y académico de primer nivel…"

Otro argumento que anima al optimismo es que España cuenta con una legislación moderna, con una fiscalía especializada y unas capacidades a nivel policial que se han adaptado a los tiempos y han evolucionado. "Personalmente además tengo la impresión de que durante la crisis sanitaria todos los actores del mundo de la ciberseguridad han dado un paso al frente, la ciberseguridad ha pasado a primer plano, si es que no lo estaba, y creo que, en general, la ciberseguridad de ciudadanos, empresas e instituciones saldrá reforzada", resume el comandante Durán.

La impunidad de estos 'agentes del mal' es un aspecto lacerante, debido a que el ciberespacio no tiene fronteras y muchos de estos activistas se parapetan en países que los protegen y hacen opacos sus ataques. En este punto, José Durán comenta que existen herramientas de cooperación policial y judicial internacional: la más importante en este ámbito es el Convenio de Budapest y que, en general, la colaboración con los países que son parte de este tratado internacional (65 en la actualidad), puede permitir llevar a buen término las investigaciones. "Fuera de este marco nos encontramos países con los que resulta más difícil trabajar, bien porque no tienen un nivel de desarrollo suficiente, o bien porque tienen concepciones distintas en lo referente a soberanía y ciberespacio". Todo ello dejando de lado la existencia de determinados grupos que operan en el ciberespacio y que muy probablemente tengan apoyos de determinados gobiernos.

El comandante Durán destaca el papel de la Europol, una agencia de la Unión Europea que apoya y coordina las investigaciones de las policías de todos los Estados Miembros. Europol gestiona un servicio de análisis de malware denominado EMAS (Europol Malware Analysis Solution) que permite a los ciberinvestigadores nacionales remitir muestras de malware y recibir un informe automático acerca de la muestra en cuestión. Pero el verdadero valor añadido del sistema es que es capaz de integrar esos informes, cruzarlos con otros generados para terceros países y encontrar vínculos entre muestras subidas en el marco de diferentes investigaciones. "Esto permite que los investigadores que trabajan en distintos países sobre una misma muestra de

malware puedan compartir información, coordinar sus investigaciones y ser más eficaces", concluye el portavoz de la Guardia Civil.

Concienciación, la mejor vacuna

Frente a este pulso en la sombra entre el bien y el mal, la sociedad y a las empresas cuentan con la concienciación como la mejor vacuna. Una asignatura pendiente, como enfatiza Penteo, consultora que ha constatado que solo el 12% de las compañías analizadas dispone de un ISMS implantado y certificado. Adrián López, digital advisor en Penteo, describe que "la crisis de Covid-19 ha sacado a relucir, de manera más plausible, esa falta de madurez en muchos ámbitos dentro de la ciberseguridad y muchas empresas han podido constatar de forma algo amarga el hecho de no disponer de un plan de continuidad de negocio, el no estar preparados técnica ni estructuralmente para proteger sus activos en un escenario de teletrabajo masivo o la carencia de esos planes directores de seguridad para hacer frente a un escenario del caos como puede darse en un ciberataque o como ha podido poner sobre la mesa una crisis como la actual".

Pero miremos la parte positiva, que el analista de Penteo subraya: "Hemos empezado a observar una mayor preocupación o conciencia por parte de nuestros clientes en los ámbitos mencionados y todo hace prever que entre finales de 2020 y 2021 aumente (aunque poco aún) la inversión TI en este tipo de proyectos". Hay trabajo por hacer, Juan Santamaría, CEO de Panda Security, afirma que la ciberdefensa tradicional ya no es válida; es necesario tener visibilidad de todos los endpoints y protegerlos con soluciones multicapa que monitoricen en tiempo real las amenazas. "Además, esos puntos deben salvaguardarse mediante un enfoque que reúna capacidades avanzadas de protección en el endpoint (EPP) y de detección y respuesta del mismo (EDR), unido a una postura de seguridad de confianza cero respaldada por inteligencia artificial", todo un círculo virtuoso para edificar el futuro. ■

"El coste medio de una brecha de datos en el sector sanitario se cotiza a 408 dólares por historial médico"