ARI 67/2020
12 de mayo de 2020

Ciberseguridad en tiempos de pandemia: repaso a la COVID-19

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

Tema

La COVID-19 ha creado una tormenta casi perfecta en el ciberespacio. El incremento de la cibercriminalidad y de la desinformación ha puesto a prueba la resiliencia de todos los actores públicos y privados.

Resumen

La COVID-19 ha demostrado que hay virus, como el SARS-CoV-2, más peligrosos para la seguridad mundial que los que rondaban por el ciberespacio. La conmoción creada por su irrupción en la rutina de la población, Administraciones y empresas ha creado una ventana de oportunidad por la que se han colado nuevos riesgos y viejos actores entre las preocupaciones de los que velan por la ciberseguridad. Sus medidas de protección, diseñadas para un crecimiento progresivo, se han visto casi desbordadas por la exposición a nuevos fenómenos como el del teletrabajo, la educación o el ocio masivos, que han aumentado su superficie de exposición en muy pocos días u horas. Este ARI analiza las manifestaciones de cibercriminalidad y desinformación asociadas a la COVID-19.

Análisis

La memoria de la ciberseguridad es corta, pero muy intensa, y conoce que los actores que generan inseguridad en el ciberespacio –las amenazas– aprovechan cualquier oportunidad para hacer daño o lucrarse con ella. Y, aunque la aparición de una pandemia era una posibilidad remota, a medida que se empezó a materializar saltaron las alarmas sobre sus implicaciones para el ciberespacio. Ya en marzo de 2020, el *CIBER Elcano* se hizo eco de los avisos de la Organización Mundial de la Salud (OMS) que avisaban de que la pandemia vendría acompañada de acciones de desinformación y cibercriminalidad para las que acabó acuñando el término de *infodemia*[1]. Los hechos han dado la razón a la OMS y la COVID-19 ha permitido desplegar a las amenazas (actores) que actúan en internet sus capacidades para desinformar sobre la crisis mundial de salud o aprovecharse de ella para ganar dinero o reputación. Junto a lo anterior, y debido a la multiplicación del uso de las redes y sistemas de información para teletrabajo, educación u ocio durante la pandemia, han aumentado los ciberataques sobre las infraestructuras críticas para la gestión de la crisis –hospitales incluidos–, así como sobre los medios improvisados de comunicación a distancia tales como Zoom que

[1] UN Department of Global Communications (2020), "UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis", https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19.

no contaban con sistemas de protección adecuados. El aumento de las conexiones y el tráfico ha puesto a prueba la resiliencia de las redes y sistemas de telecomunicaciones, con distintos resultados según la mayor o menor capacidad de las infraestructuras disponibles, por lo que se hace necesario pensar cómo se van a gestionar en el futuro las nuevas necesidades.

El tráfico se dispara

Los operadores de telecomunicaciones conocen el comportamiento del tráfico en situaciones de crisis (atentados o desastres familiares), en eventos familiares o días festivos señalados (Nochevieja, Día de la Madre) o en horas de máxima audiencia (*prime time*), por lo que diseñan las redes para atender a los picos de demanda y evitar el colapso del sistema[2]. Estas previsiones se desbordaron desde el principio y, según datos recogidos de diversas fuentes por el Observatorio Nacional 5G para los primeros días de la crisis, Nokia detectó crecimientos de hasta el 40% en las regiones más afectadas por la pandemia, WhatsApp duplicó su tráfico en las horas laborables y lo quintuplicó en la tarde del primer festivo y la demanda de Netflix se duplicó en las primeras mañanas y creció las primeras horas de la tarde (27-42%)[3].

El funcionamiento de internet no se ha interrumpido, pero se ha visto ralentizado en ocasiones por la alta demanda en determinadas franjas horarias, lo que ha producido inestabilidad o perturbación del tráfico en algunas ciudades y áreas geográficas que no estaban dotadas de la cobertura digital idónea. Las transmisiones en directo y la reproducción masiva de vídeos han puesto las redes y sistemas al límite de sus posibilidades para atender las demandas adicionales de la docencia, los negocios o el ocio, por lo que se han tenido que adoptar algunas medidas preventivas para preservar el funcionamiento de internet. El Reglamento UE 2015/2020 prohíbe a los operadores bloquear, ralentizar o priorizar el tráfico como norma general, pero les permite adoptar medidas técnicas de carácter excepcional para prevenir la congestión inminente de internet, siempre de acuerdo a los principios de no discriminación, trasparencia y limitación en el tiempo. En consecuencia, la Comisión Europea y el órgano de reguladores europeos de comunicaciones electrónicas (BEREC) apelaron a los operadores de telecomunicaciones y a los proveedores de servicios digitales en un comunicado conjunto a cooperar con las autoridades nacionales en la supervisión del tráfico para evitar la congestión. Dentro de las medidas preventivas adoptadas se encuentran, entre otras conocidas en la UE, la reducción de la calidad de la transmisión en directo (streaming) de Netflix y YouTube a petición del comisario Thierry Breton[4].

[2] El colapso también se puede atender bloqueando el tráfico o discriminando unos flujos frente a otros, pero entonces ya no sería una internet abierta.

[3] Observatorio Nacional 5G, “Networks respond favorably to traffic growth due to Covid-19”, 6/IV/2020, https://on5g.es/en/networks-respond-favorably-to-traffic-growth-due-to-covid-19.

[4] Aproximadamente, el vídeo ocupa dos terceras partes del tráfico en la UE, Netflix una cuarta parte y Google y Facebook la quinta parte. Hadas Gold (2020), “Netflix and YouTube are slowing down in Europe to keep the internet from breaking”, *CNN Business*, 20/III/2020, https://edition.cnn.com/2020/03/19/tech/netflix-internet-overload-eu/index.html.

Medidas como la anterior han funcionado, aunque no hubieran sido tan necesarias si toda la UE dispusiera de la capacidad y calidad de infraestructuras de fibra óptica como España[5], lo que confirma la necesidad de impulsar la estrategia y políticas de banda ancha como las de la UE y, en particular, el plan de acción para el despliegue de las redes 5G, que fijaba como objetivo incrementar la cobertura mínima (30 megabytes por segundo para toda la población y 100 megabytes para la mitad de los hogares en 2020). Lo que antes era un problema de desigualdad en el disfrute de los beneficios de la economía digital, tras la COVID-19 es, además, un problema de seguridad.

La desinformación que no cesa

El Servicio Europeo de Acción Exterior (SEAE), en un informe reciente, se ha hecho eco de las campañas de desinformación coincidentes con la COVID-19[6]. Son campañas que ponen en riesgo a la población afectada y perjudican la imagen de los sistemas sanitarios y la gestión de la crisis en la UE. Entre otras señaladas en el informe, además de las clásicas negacionistas de la pandemia o las conspirativas, figuran las que atribuyen virtudes curativas a la leche¸ el vodka o la medicina tradicional y se las niegan a las vacunas y fármacos. Su circulación genera reacciones incontroladas; por ejemplo, las manifestaciones violentas en Reino Unido, Bélgica y Países Bajos contra las redes 5G en las que se quemaron torres[7]. Mientras medios de comunicación públicos y privados afines al Kremlin continúan aprovechando la COVID-19 para deteriorar la imagen europea, sus homólogos chinos hacen lo propio magnificando su respuesta en comparación con la europea[8]. Y, si no lo hacen los Estados, lo hacen sus seguidores –voluntarios o subvencionados– para alimentar la tensión geopolítica, incluso en situaciones tan complicadas como una pandemia, mediante la movilización de troles que defienden sus causas patrióticas y desacreditan las de los rivales, con lo que generan confusión y ruido, aunque su impacto real esté aún por demostrar[9]. No obstante, el mayor riesgo de la desinformación es poner en duda las recomendaciones de la OMS, la credibilidad de las medidas de protección o respuesta frente a la COVID-19, mediante señuelos como los que revela Fortinet.

[5] Europapress (2020), “España, líder europeo en despliegue de fibra óptica por delante de Alemania, Francia o Reino Unido”, 19/III/2020, https://www.europapress.es/portaltic/sector/noticia-espana-lider-europeo-despliegue-fibra-optica-delante-alemania-francia-reino-unido-20200319113712.html.

[6] División de Comunicaciones Estratégicas y Análisis de la Información del SEAE, actualización del informe, 29 de abril de 2020.

[7] Nic Fildes, Mark Di Stefano y Hannah Murphy (2020), “How a 5G coronavirus conspiracy spread across Europe”, *Financial Times*, 16/IV/ 2020, https://www.ft.com/content/1eeedb71-d9dc-4b13-9b45-fcb7898ae9e1.

[8] Sarah Cook describe la compra china de anuncios y tribunas en medios importantes de comunicación occidentales en “Beijing’s Coronavirus Propaganda Has Both Foreign and Domestic Targets”, Freedom House, 20/IV/2020, https://freedomhouse.org/article/beijings-coronavirus-propaganda-has-both-foreign-and-domestic-targets.

[9] Elise Thoran y Ahbert Zhaneg (2020), “Covid-19 Attracts Patriot Troll Campaigns”, Australian Strategy Policy Institute (ASPI), 17/IV/2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-04/Patriotic%20Troll%20Campaigns%20Report_ASPI%20Cyber.pdf?3UM1P9V4gVpAacBYaf7zxRM9HMla.twV; Andrés Ortega, “Bots rusos: mucha injerencia, ¿poca influencia?”, Blog Elcano, 28/IV/2020, https://blog.realinstitutoelcano.org/bots-rusos-mucha-injerencia-poca-influencia/

Las grandes plataformas vienen colaborando en la gobernanza de internet y de las redes sociales[10] para anticiparse a las demandas de los reguladores y contrarrestar las críticas a las malas prácticas de su posición dominante. Comienzan a tomar conciencia de que los efectos masivos de la desinformación no serían posibles sin la difusión a través de ellas, lo que las obliga a multiplicar sus capacidades de contrastar los hechos y evitar su difusión. Además de la lucha contra la desinformación, los delitos de odio o la explotación infantil, entre muchas otras que han seguido llevando a cabo, lo novedoso de su actuación en la COVID-19 es que han tenido que detectar anuncios que ofrecían productos sanitarios falsos o especulativos o que ponían en riesgo la salud de la población y cerrar las cuentas. También han tenido que afrontar problemas con la ingente verificación de contenidos, por ejemplo, en los vídeos con anuncios de publicidad, lo que ha ralentizado su autorización y dificultado su monetización. En todo caso, y con los datos conocidos hasta ahora, parece que las grandes plataformas han tomado medidas más agresivas que en ocasiones anteriores, más controvertidas por su relación con la libertad de expresión o las campañas electorales[11].

Ciberataques a discreción

Contra toda esperanza, las amenazas del ciberespacio han aprovechado la COVID-19 para intensificar sus ataques deliberados contra infraestructuras críticas como las de los hospitales, contra quienes se han visto obligados al teletrabajo y contra quienes temen o están interesados en las noticias relacionadas con la pandemia. Los ciberataques se han dirigido contra altos dirigentes de la OMS haciendo públicas sus contraseñas y direcciones de cuentas –aunque es posible que se hayan obtenido anteriormente– o intentando suplantar su identidad. También contra los sistemas y equipos de la OMS implicados en la gestión de la crisis desplegados en algunos Estados, según informaron a la organización las autoridades de ciberseguridad de varios países de la UE, Israel, Suiza, Microsoft o Interpol[12].

El alto representante de la UE, Josep Borrell, emitió una declaración en la que denunciaba la multiplicación de los ataques contra operadores esenciales, incluidos los de salud, desde el inicio de la pandemia. En el mismo sentido, el Banco Central Europeo alertó al sistema financiero sobre los riesgos para la ciberseguridad y las medidas de contingencia que adoptar frente a la COVID-19. Fuera de Europa, el Departamento de Defensa de los EEUU. ha tenido que articular un grupo de trabajo (COVID-19 Telework Readiness Task Force) para prevenir las vulnerabilidades creadas por el trabajo a

[10] Ángel Badillo, "La sociedad de la desinformación: propaganda, 'fake news' y la nueva geopolítica de la información", DT 8/2019, Real Instituto Elcano, 14/V/2019, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion.

[11] Twitter, "Staying safe and informed on Twitter", 3 de abril de 2020, https://blog.twitter.com/en_us/topics/company/2020/covid-19.html; Facebook, "Keeping People Safe and Informed about the Coronavirus", 22 abril de 2020, https://about.fb.com/news/2020/04/coronavirus/#joint-statement.

[12] Ryan Gallaher, "Hackers Target Top Officials at World Health Organization", *Bloomberg*, 21/IV/2020, https://www.bloomberg.com/amp/news/articles/2020-04-21/top-officials-at-world-health-organization-targeted-for-hacks.

distancia, pero también para preservar el mismo grado de eficacia en las infraestructuras de seguridad nacional con las que están interconectadas las fuerzas armadas.

El interés por donar o solicitar fondos de ayuda para los afectados ha sido otro de los incentivos explotados por los ciberdelincuentes. Los intentos de estafa para aprovechar el altruismo o la necesidad se han sucedido explotando el miedo y la desprotección o falta de pericia digital de los beneficiarios. Se han creado dominios ficticios para atraer las donaciones suplantado la identidad de organizaciones privadas de caridad y públicas de asistencia o simplemente se ha proporcionado información sobre la pandemia para infectar los ordenadores con *malware*[13]. La multiplicación de lugares de trabajo domésticos sin las adecuadas medidas corporativas de protección ha sido otro blanco rentable para ciberataques y estafas. Las amenazas no han dudado en buscar los puntos débiles de las cadenas ampliadas de teletrabajo, que han aumentado la superficie de exposición de las Administraciones y empresas con multitud de aplicaciones, equipos y procedimientos de trabajo a distancia sin la debida supervisión de los responsables de la seguridad y la información de las actuaciones de las organizaciones para las que trabajan.

Algunas agencias, como el FBI, han identificado centenares de páginas web implicadas en el fraude que suplantan la identidad de organizaciones sanitarias (públicas y privadas) vinculadas a la gestión de la COVID-19 para hacerse con las claves o el dinero de las ayudas. También han alertado de ello centros nacionales de ciberseguridad como el del Reino Unido y el de los EEUU.[14] El fraude era fácil porque, según una encuesta de la IBM-X Force de abril, aproximadamente la mitad de los consultados esperaban recibir algún tipo de notificación relacionada con la COVID-19 o estarían dispuestos a abrir alguna relacionada con los test o las ayudas disponibles. Dadas las expectativas, el tráfico de *spam* malicioso se incrementó en más del 6.000% en el mes de abril de 2020[15]. En el mismo sentido, Google reconoció que había tenido que filtrar y bloquear una cantidad ingente de correos (18 millones diarios) y *spam* (240 millones diarios) de Gmail que trataban de suplantar la identidad de agencias, organizaciones y empresas de reparto (en 2019 Google bloqueó y suprimió 2.700 millones de anuncios y clausuró un millón de cuentas de anunciantes, lo que da una idea del incremento debido a la COVID-19)[16]. Además del incremento cuantitativo, el vicepresidente de la compañía, Scott Spencer, resalta la capacidad de adaptación de la cibercriminalidad y el nivel de sofisticación de las tácticas con el que las amenazas han tratado de superar las medidas de control de su plataforma.

[13] Rachel Siegel, "Data breach may have exposed information of thousands of SBS emergency loan applicants", *The Washington Post*, 23/IV/2020, https://www.cuinsight.com/data-breach-may-have-exposed-personal-information-of-thousands-of-sba-emergency-loan-applicants.html.

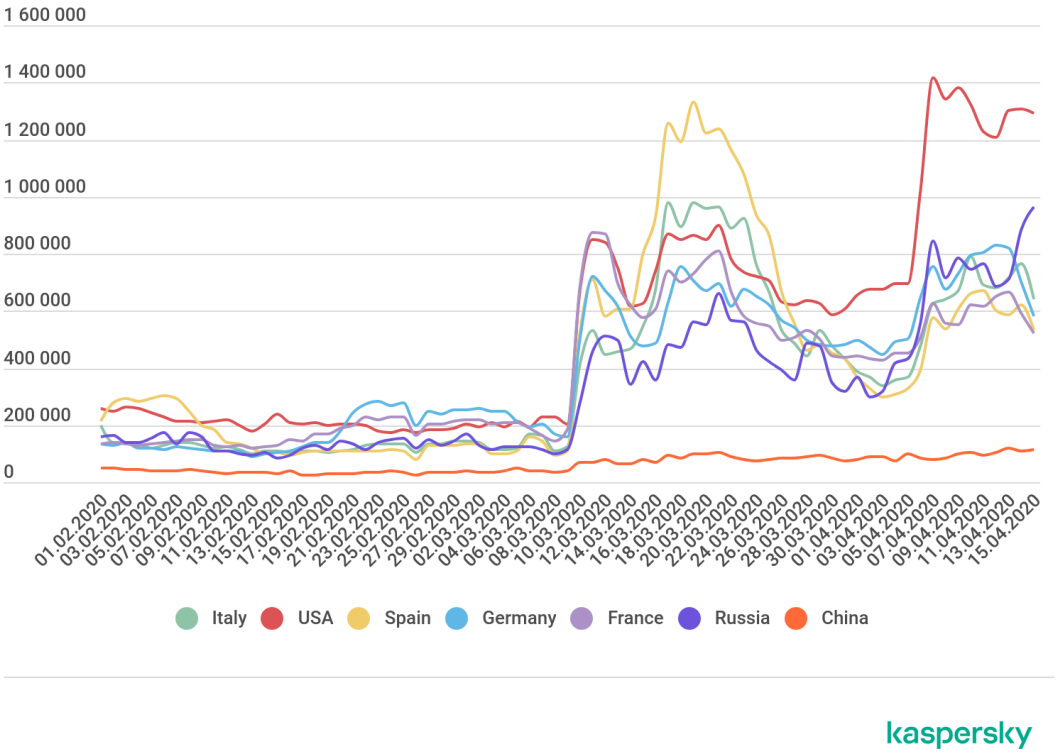
[14] National Cyber Security Centre (NCSC), "Advisory: Covid-19 exploited by malicious cyber actors"; Europol, https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf; "Staying safe during Covid-19: what you need to know"; Interpol, "Covid-19. Stay Safe", https://www.interpol.int/es/Como-trabajamos/COVID-19.

[15] IBM Security, "2020 Consumer Small Business Covid-19 Awareness Study", 7-8 de abril de 2020, https://www.ibm.com/downloads/cas/ZVNNJNQJ.

[16] Google Threats Analysis Group, "Findings on Covid-19 and online security threats", 1 de mayo de 2020, https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats.

La proliferación del teletrabajo desencadenó una oleada de ciberataques sobre los protocolos de Microsoft para acceder al control remoto de las ordenadores de trabajo (RDP), según Kaspersky. Aprovechando la confusión creada por el teletrabajo masivo y las dificultades para parchear los terminales conectados remotamente, los ciberataques pasaron de algunos centenares de miles por día a rozar el millón y superarlo en países como España y Estados Unidos, como refleja la Figura 1.

Figura 1. Ciberataques diarios sobre los protocolos de control remoto (RDP)



Fuente: Kaspersky, 29/IV/2020, https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/.

No han faltado repuntes en actividades criminales como la explotación infantil. Los cibercriminales han aprovechado el incremento del tráfico para circunvenir los controles de las grandes plataformas empleando lenguaje cifrado para facilitar a los pedófilos enlaces encubiertos (“CP” para *child pornography* o “caldo de pollo”). El repunte ha obligado a las grandes plataformas a desarrollar nuevos mecanismos de detección y llevar a cabo esfuerzos adicionales, pero los cibercriminales continúan distribuyendo sus códigos de captación a través de plataformas con menor capacidad de detección, como WhatsApp, Mega o TamTam[17].

[17] Olivia Solon, “Child sexual abuse images and online exploitation surge during pandemic”, *NBC news*, 23/IV/2020, https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506.

La proliferación de nueva amenazas también ha proporcionado una ventana de oportunidad a muchas compañías de ciberseguridad, como Thales o IBM, que han aprovechado para editar recomendaciones e incluso ofrecer servicios gratuitos a sus clientes de siempre o a los potenciales de los nuevos grupos en riesgo. Del lado público, en España instituciones oficiales como el CCN-CERT o el Incibe han alertado sobre las distintas modalidades maliciosas y publicado boletines informativos a medida que se conocían nuevas malas prácticas[18]. Entre dichas informaciones, merecen atención algunas recomendaciones y buenas prácticas para el uso de aplicaciones en ámbitos emergentes de comunicación *online* como las videoconferencias, el ocio y la docencia, como Zoom. La pandemia ha provocado un uso intensivo de las infraestructuras y los servicios para facilitar la comunicación, el entretenimiento o la enseñanza no presencial, que probablemente aprovecharán el impulso para consolidarse en el ciberespacio.

Conclusiones

Todavía es demasiado pronto para disponer de datos que evalúen el impacto de la COVID-19 sobre la ciberseguridad. Los datos presentados son un anticipo de los que tienen que seguir y se refieren a datos disponibles en fuentes abiertas, por lo que se precisará tiempo y trasparencia antes de conocer el alcance real sobre el sector público, especialmente los datos sobre las organizaciones implicadas en la gestión de la pandemia.

Internet, las infraestructuras y los sistemas de información han demostrado una notable capacidad de resiliencia, aunque con daños colaterales menores en algunos servicios y zonas geográficas. Los responsables de la seguridad de la información tendrán que aprender de la experiencia para subsanar las debilidades en el futuro.

Las pandemias han venido para quedarse, por lo que urge llevar a cabo un amplio esfuerzo de reflexión colectiva para evaluar las medidas que tomar si aparece un nuevo brote. Pero, como no ha producido el temido fallo sistémico, es probable que los responsables de la ciberseguridad no aprendan todas las lecciones posibles de la COVID-19 y consideren que las medidas de resiliencia actuales les volverán a servir en la siguiente pandemia, un error en el que no incurrirán los actores que han puesto a prueba la resiliencia de la sociedad digital, quienes han demostrado su capacidad de adaptación y volverán a intentarlo.

[18] Incibe, “Cómo detectar y prevenirse ante los fraudes y bulos que circulan en relación al COVID-19”, 27 de marzo de 2020, https://www.incibe.es/sala-prensa/notas-prensa/detectar-y-prevenirse-los-fraudes-y-bulos-circulan-relacion-al-covid-19; CCN-CERT, “Repunte de las campañas de phishing relacionadas con la pandemia COVID-19”, 19 de marzo de 2020, https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9716-ccn-cert-al-05-20-repunte-campanas-de-phishing-por-covid-19.html.