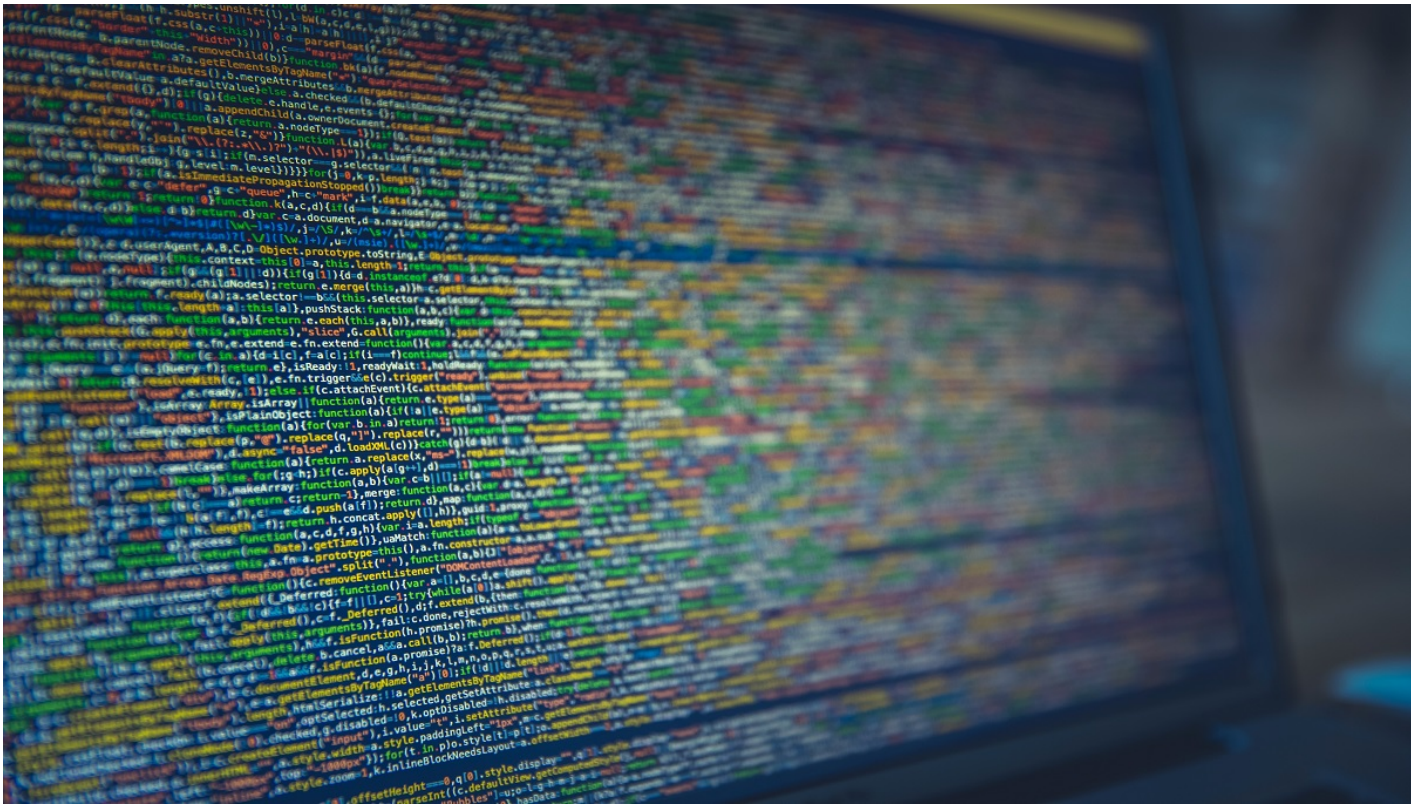
Cuanto más digitales, más expuestos y vulnerables ante las ciberamenazas

La crisis sanitaria nos ha obligado a depender más de la tecnología haciéndonos más vulnerables ante las ciberamenazas



por Pablo Rodríguez Canfranc

La pandemia nos ha obligado a introducir la tecnología más intensivamente en nuestras vidas. En las últimas semanas gran parte de nuestro trabajo y de nuestro ocio se ha volcado más en las redes. La confusión e incertidumbre reinantes, así como la falta de formación e información sobre aspectos relacionados con la ciberseguridad nos hacen muy vulnerables ante los delincuentes que campan por internet.

Una enfermedad contagiosa ha puesto el mundo cabeza abajo. Una parte importante de la población del planeta se ha visto obligada a confinarse en su domicilio. La economía global se ha parado en seco y su recuperación será lenta y dolorosa. El ciudadano se enfrenta a un cúmulo de sensaciones que van desde la incredulidad –“esto no puede estar pasando”-, hasta el miedo y la indefensión. En lo que todos parecen coincidir es que las cosas ya no volverán a ser como eran antes de esta crisis: emerge un nuevo paradigma, cuya forma aún desconocemos. Y, por supuesto, la confusión e incertidumbre que se ha apoderado de la sociedad son aliadas naturales de la ciberdelincuencia, que se ha encontrado con un escenario idóneo para llevar a cabo ciberataques exitosos, tanto con fines de lucro económico, como con objetivos políticos, geoestratégicos o ideológicos.

La súbita “digitalización extrema” a la que hemos tenido que adaptarnos ha jugado abiertamente a favor del hacker, principalmente porque ahora estamos más expuestos tecnológicamente hablando. La sociedad se ha hecho mucho más dependiente de las infraestructuras digitales y la conectividad. Además, nos hemos visto abocados al teletrabajo, sin que gran parte de las empresas y organizaciones hayan podido probar debidamente cómo implantar con éxito esta modalidad. Por otro lado, el consumo electrónico se ha disparado: todo lo que hacemos encerrados tiene un mayor peso digital. Finalmente, existe un amplio porcentaje de población que no está tan familiarizado con el uso cotidiano de tecnología, pero que se ha visto igualmente empujado a incorporarla en su vida diaria. Desde la perspectiva de cazador del ciberdelincuente, la pandemia ha multiplicado el número de presas que se encuentran completamente al descubierto y que son muy fáciles de abatir.

En el lado corporativo, la experiencia pasada demuestra que el empleado siempre es el eslabón más débil en la estrategia de ciberdefensa de la empresa. Los delincuentes hacen uso de lo que se conoce como ingeniería social, o el manipular y explotar la psicología de las personas con el fin que revelen información sensible o que den acceso a sistemas informáticos. Generalmente, la ingeniería social la llevan a cabo lanzando cebos a la víctima potencial, ofreciendo algo atractivo para conseguir que se descargue archivos maliciosos, o intentan engañarla con correos electrónicos falsos, por ejemplo, suplantando a su banco para obtener las claves de acceso a sus cuentas. Somos vulnerables. Así lo veía Elliot Anderson, el hacker protagonista de la serie *Mr. Robot*: “nunca me ha costado *hackear* a la mayoría de la gente. Si les escuchas, si les observas, sus vulnerabilidades son como una señal de neón atornillada a sus cabezas”.

Si antes de la llegada del COVID-19 la formación relacionada con la ciberseguridad era relevante, ahora, cuando el teletrabajo es la norma, se ha vuelto indispensable. El trabajador ya no se encuentra protegido tras los cortafuegos y muros de la empresa, sino que opera en la soledad de su domicilio conectado a un *router* doméstico, con un nivel de seguridad entre bajo y nulo.

> **“ Así lo veía Elliot Anderson, el hacker protagonista de la serie Mr. Robot: nunca me ha costado hackear a la mayoría de la gente. Si les escuchas, si les observas, sus vulnerabilidades son como una señal de neón atornillada a sus cabezas ”**

No nos engañemos, los ciudadanos de la calle andamos todos muy escasos de conocimientos de seguridad. Las conexiones que tenemos en casa suelen tener una seguridad insuficiente, y a menudo incluso no protegemos el acceso a la red wifi domestico con contraseñas robustas para evitar que puedan entrar intrusos en ella. Por otro lado, todos los dispositivos familiares que conectamos a dichas redes –portátiles, teléfonos, tabletas, consolas- tampoco suelen tener actualizadas las últimas versiones del software, lo que genera fallos importantes de seguridad. Si a ello le sumamos que carecemos, en términos generales, de las nociones básicas de ciberseguridad, podemos comprender que esta situación de confinamiento expone a las ciberamenazas, no sólo a las familias, sino a las empresas, cuyos sistemas pueden verse atacados a través de las brechas de seguridad que presenta el entorno doméstico del teletrabajador.

El denominado Ataque de día cero (*zero-day attack*) adquiere connotaciones más peligrosas en este formato de trabajo en remoto. Se trata de una agresión que aprovecha una vulnerabilidad en una aplicación o sistema, que ha

sido detectada por el atacante antes que por el dueño, para introducir código malicioso en el intervalo de tiempo previo a su localización y reparación mediante un parche informático. En el caso de un particular, este tipo de vulnerabilidad puede mantenerse sin ser descubierta –al no contar este con los servicios adecuados de ciberseguridad- dejando permanentemente abierta la puerta a los intrusos.

Los ataques del coronavirus

Las cifras de ciberataques se han disparado en las últimas semanas. La media diaria es de 2 600 ataques, pero el día 28 de marzo llegaron a registrarse hasta 5 000. Con todo, los expertos avisan de que el pico de actividad maliciosa probablemente no se ha alcanzado todavía. Las acciones detectadas son de todo tipo: desde intentos de robo de contraseñas y datos, hasta ataques directos contra organizaciones, e incluso, hospitales. También se ha producido una escalada del volumen de bulos y noticias falsas en circulación relacionadas con la pandemia, cuyo fin es crear pánico entre la población y desestabilizar las instituciones.

Una de las modalidades más utilizadas durante esta crisis de la pandemia de ataque es el *phishing* utilizando COVID-19 como señuelo. Se trata del envío de correos fraudulentos, generalmente suplantando a una organización u autoridad, con el fin de que el destinatario acceda a un enlace web malicioso o que entregue información personal, como, por ejemplo, contraseñas de acceso a determinados servicios. El éxito de este formato está relacionado con la incertidumbre que provoca esta situación que vivimos y el ansía de información que a todos nos genera.

Recientemente, los delincuentes han distribuido programas maliciosos (*malware*) suplantando al Ministerio de Salud chino, y también han fingido dirigirse en nombre de la Organización Mundial de la Salud (OMS) solicitando donaciones en bitcoins para sufragar la investigación para luchar contra el virus. En Estados Unidos los ciberatacantes aprovechan los rumores en su propio beneficio, y, aunque no se había producido ningún comunicado oficial por parte del Gobierno, realizaron un envío de mensajes anunciando una ayuda estatal de 1 000 dólares para aliviar la situación económica de las familias, que contenía un enlace web para solicitarla, que, por supuesto, era malicioso.

Otro ejemplo del uso de la ingeniería social a través del *phishing* en tiempos de pandemia ha sido la creación de una web con un mapa interactivo de la difusión del coronavirus por el mundo, que los delincuentes fingían que pertenecía a la John’s Hopkins University, una institución sanitaria de prestigio. Cuando el navegante accedía a la dirección *corona-virus-map[dot]com*, su dispositivo era infectado por el troyano AZORult, un *malware* que roba datos personales de la víctima para su venta en el mercado negro[1].

> **“ Los delincuentes han distribuido programas maliciosos (malware) suplantando al Ministerio de Salud chino, y también han fingido dirigirse en nombre de la Organización Mundial de la Salud (OMS) ”**

La organización de ciberseguridad británica National Cyber Security Centre ha llegado a detectar actividades de *phishing* a través de SMS en vez de correo electrónico, algo poco frecuente. En este caso, el mensaje se hacía pasar por un comunicado del Gobierno inglés para solicitar subvenciones de cara a afrontar los daños económicos causados por la pandemia.

La difusión de *malware* o programas maliciosos es otra de las prácticas habituales entre las ciberamenazas, y por supuesto ha estado de plena actualidad en la crisis del COVID-19. Generalmente, este tipo de práctica tiene por objeto infectar con virus informáticos los equipos, y, en ocasiones, bloquear y encriptar la información de la víctima con el objeto de pedir un rescate monetario para devolverla. Esto último es lo que se conoce como *ransomware*. Durante la pandemia este tipo de acciones delictivas han sido disfrazadas de información relacionada con el coronavirus. Los programas maliciosos se hacen pasar por archivos inofensivos, con extensiones pdf, mp4 o docx, de forma que cuando la confiada víctima los abre, su dispositivo queda infectado automáticamente.

El equipo de Respuesta a Incidentes de ITS Security ha podido identificar numerosas campañas activas en este campo, como la de *ransomware* con los virus NetWalker y Ryuk contra el sector sanitario, que envía correos electrónicos al personal para conseguir infectar el sistema informático de los hospitales. El sector sanitario es un objetivo tradicional de los ciberdelincuentes, porque sus sistemas guardan datos muy sensibles de los pacientes y porque es un servicio esencial para la comunidad, por lo que es indispensable mantener su funcionamiento. De ahí que sufra con frecuencia intentos de extorsión vía *ransomware*, como el que sufrió el Hospital Universitario de Torrejón, en Madrid, en enero de este año, que afectó la disponibilidad de varios de sus sistemas informáticos.

Por su parte, los troyanos habituales TrickBot y Emotet ahora incorporan textos relativos al COVID-19, en un intento de enmascararse y sortear los programas antivirus. Otro ejemplo de *ransomware* es el troyano Kpot Infostealer, que también se disfraza con textos relativos al coronavirus, cuya finalidad es robar información. BLACK WATER es un troyano de “puerta trasera”, que, simulando ser información sobre COVID-19, instala el malware cuando la víctima ejecuta el archivo “Importante – COVID-19.docx.exe”, que simula ser un archivo de texto del procesador Word de Microsoft, pero es realmente un programa (.exe).

Finalmente, en el terreno financiero ITS Security destaca troyanos como GIMP y CERBERUS, que utilizan el coronavirus para atacar a sus víctimas, instalando en sus dispositivos *malware* para robar datos de acceso a las aplicaciones bancarias.

El uso de mapas sobre la propagación de la enfermedad por el mundo no se limita al caso anteriormente expuesto de la John’s Hopkins University. ITS advierte del peligro de CovidLock, una acción de ransomware con forma de *app* que promete mantener actualizado al usuario que la instala en su móvil sobre la difusión del COVID-19 en su región y en el mundo. Sin embargo, una vez instalada bloquea la pantalla de inicio y solicita un rescate a cambio de liberarla.

La importancia de concienciar a la ciudadanía

La lista de ciberataques y amenazas sigue y además aumenta cada día. Los sistemas de protección son fundamentales, pero somos cada uno de nosotros los elementos fundamentales de la estrategia de ciberseguridad. Debemos aprender de la experiencia que estamos viviendo y sistematizar las enseñanzas, no solo ya ante la posibilidad de que se desencadene una nueva crisis, sino para enfrentar nuestra vida digital cotidiana, que día a día se enfrenta a amenazas cada vez más sutiles y peligrosas. Y como ciudadanos digitales, es nuestro deber formarnos e informarnos para impedir, en la medida de lo posible, caer en las trampas que nos ponen los *hackers*.

No obstante, en Europa se detecta una notable falta de información sobre los riesgos del cibercrimen. Únicamente el 46% de los ciudadanos europeos se considera bien informado, de acuerdo con los datos del Eurobarómetro. Y este porcentaje disminuye al 35% en el caso de los españoles.

> **“ Tan solo el 45% de los europeos ha optado por instalar un antivirus o modificar el que ya poseía ”**

Atendiendo a la aplicación de medidas de seguridad, tan solo el 45% de los europeos ha optado por instalar un antivirus o modificar el que ya poseía. El 39% se muestra menos dispuesto que la media a dar información personal en páginas web. El 36% solo utiliza su propio ordenador y el 35% sólo abre correos electrónicos de personas o direcciones que conoce. En nuestro país, la instalación de antivirus es la medida de seguridad más utilizada, aunque solo alcanza al 35% de los internautas. Por otro lado, somos uno de los Estados miembros, junto a Rumanía y Portugal, en el que más porcentaje de internautas (22%) declara no adoptar ninguna medida de seguridad cuando utilizan internet.

Foto de **Markus Spiske** en **Pexels**

Notas

[1]**Crane, C.** (2020) "Coronavirus Scams: Phishing Websites & Emails Target Unsuspecting Users" en Hashed Out. Disponible en: https://www.thesslstore.com/blog/coronavirus-scams-phishing-websites-emails-target-unsuspecting-users/

Bibliografía

Basque Cybersecurity Center (2020) "La ciberseguridad en tiempos del COVID-19, más importante que nunca". Disponible en: https://www.basquecybersecurity.eus/es/actualidad-bcsc/ciberseguridad-tiempos-covid-importante-nunca.html

European Union (2017) "Special Eurobarometer 464a: Europeans' attitudes towards cyber security". Portal de datos abiertos de la UE. Disponible en: https://data.europa.eu/euodp/es/data/dataset/S2171_87_4_464A_ENG

European Union (2017) "Special Eurobarometer 460: Attitudes towards the impact of digitisation and automation on daily life". Portal de datos abiertos de la UE. Disponible en: https://data.europa.eu/euodp/es/data/dataset/S2160_87_1_460_ENG

Howell, D. (2020) "Cybersecurity In a Post-COVID-19 World" en *Silicon*. Disponible en: https://www.silicon.co.uk/security/cybersecurity-in-a-post-covid-19-world-338889

IT Reseller (2020) "Detectados 2.600 ataques diarios con temática del Covid-19". Disponible en: https://www.itreseller.es/seguridad/2020/04/detectados-2600-ataques-diarios-con-tematica-del-covid19

ITS (2020) "Informes de Ciberseguridad Especial COVID-19". Ibermática.

Mouton, F. y Coning, A. de (2020) "COVID-19: Impact on the Cyber Security Threat Landscape". ResearchGate.

National Cyber Security Centre (2020) "Advisory: COVID-19 exploited by malicious cyber actors". Disponible en: https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

Tarun, R. (2020) "COVID-19 Social Engineering Attacks" en *CSO*. Disponible en: https://www.csoonline.com/article/3533339/covid-19-social-engineering-attacks.html