Expediente N.º: EXP202401479

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento a través de prensa de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos.

Con fecha 26 de enero de 2024, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) para investigar a ORANGE ESPAGNE, S.A.U. con NIF A82009812 (en adelante, ORANGE) en relación con los siguientes hechos:

"Como consecuencia de las noticias aparecidas en los medios de comunicación, esta Agencia ha tenido conocimiento de una posible quiebra de seguridad que podría haber afectado a la compañía Orange Espagne, S.A.U. y que habría dejado la información de muchos de sus clientes expuesta y susceptible de ser utilizada con fines fraudulentos. Entre los datos que han podido quedar expuestos se incluiría el nombre, los apellidos, la dirección postal, el teléfono, el correo electrónico, el DNI, la fecha de nacimiento, la nacionalidad y el código IBAN de la cuenta corriente de los clientes.

Según las noticias publicadas, la compañía envió una comunicación a todos los posibles afectados para avisarles de lo sucedido, aconsejando a sus usuarios que durante los siguientes meses tuvieran especial precaución con los correos electrónicos, mensajes o llamadas de los cuales no pudieran confirmar su procedencia o remitente, especialmente aquellos que solicitasen información bancaria o credenciales. También, advertía a sus clientes que revisaran de manera regular la información que circulaba sobre ellos en Internet para detectar un posible uso fraudulento de sus datos privados."

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Por parte del inspector se obtienen evidencias de varias noticias publicadas en distintos medios de comunicación y redes sociales en relación con una posible brecha de seguridad sufrida por ORANGE.

De las noticias analizadas destacan como relevantes las siguientes evidencias:

Se capturan varias publicaciones realizadas en TWITTER a través de la cuenta ******CUENTA.1*** donde se difunden pruebas de haber obtenido a raíz de filtraciones públicas, las credenciales de ORANGE para acceso a RIPE NNC (Centro de Coordinación de Redes IP Europeas), haber conseguido entrar en la aplicación y realizar modificaciones en el sistema de enrutamiento.

Varias noticias publicadas en distintos portales web sobre un fallo repentino sufrido por ORANGE que dejó sin conectividad a muchos de sus clientes de la entidad y que resultó ser fruto del secuestro de la cuenta de ORANGE en RIPE NCC. De las noticias publicadas se extraen las siguientes afirmaciones relevantes para la investigación:

"*El ataque a Orange implicó la manipulación del sistema de enrutamiento de Internet conocido como BGP (Border Gateway Protocol). El atacante obtuvo las credenciales de Orange en RIPE NCC y eso le permitió redirigir el tráfico de Internet de los clientes de Orange, lo que provocó fallos al acceder a webs y aplicaciones. Este método es conocido como hijacking de BGP. Implica tomar el control de las rutas de tráfico online para poder interceptar los datos que circulan por ellas o, como en este caso, redirigirlas.*"

"*Orange no ha dado detalles sobre este ataque, pero una teoría no confirmada sugiere que el atacante robó las credenciales de la cuenta en RIPE NCC mediante un ataque de phishing a un empleado de la operadora en septiembre de 2023. Este ataque inyectó un software malicioso (infostealer) que le permitió lograr el usuario y la contraseña de esa cuenta. Según los detalles publicados, se trataría de una contraseña extremadamente simple y carente de una verificación de doble factor, lo que permitió que el atacante pudiese acceder únicamente con la contraseña.*"

En relación con las noticias publicadas en los distintos medios de comunicación, todas ellas hacen referencia a un posible ataque sufrido por ORANGE a partir del cual se filtraron las credenciales de acceso a RIPE NCC de la compañía; no obstante, en ninguna de estas se hace referencia a la posible afectación de datos personales provocado por este ataque. Se destacan las siguientes publicaciones:

******URL.1***
******URL.2***
******URL.3***

Ante las dudas suscitadas sobre la posible afectación a datos personales a raíz del incidente de seguridad sufrido por ORANGE, en fecha 5 de marzo de 2024 se realiza un primer requerimiento de información dirigido a este responsable de tratamiento y marcado por la siguiente línea de investigación:

- Solicitar el registro documentado del incidente e información detallada del incidente.
- Investigar las causas que hicieron posible el incidente, la posible afectación de datos personales, su posible filtración y sus consecuencias.

En fecha 13 de marzo de 2024 se recibe respuesta al requerimiento anterior, de su análisis se extrae la siguiente información relevante:

- "*La incidencia se originó debido a un acceso no autorizado a la web de RIPE por parte de un usuario no autorizado. RIPE es una base de datos técnica, donde solo parecen datos administrativos técnicos de telecomunicaciones para enrutar el tráfico en internet. A través de RIPE no se acceden, ni directa ni indirectamente, a datos de carácter personal*. *A excepción de la aplicación RIPE, el atacante no logró acceso a ninguna de las aplicaciones cuyas credenciales pudiera haber obtenido. No obtuvo acceso al contenido del PC infectado, ni a la información que en él se pudiera encontrar"*.
- *"Las aplicaciones cuyas credenciales pudieron haberse obtenido son de carácter técnico con información de despliegues, replanteos, infraestructura de red, etc. sin que a través de ellas se pueda tener acceso a información personal. No hay ninguna evidencia sobre accesos no autorizados; no hay evidencias que se hayan utilizado ninguna de las credenciales obtenidas; en las aplicaciones no se advierten picos de actividad, siguiendo un patrón de actividad normal del servicio.*"
- *"No se ha producido una violación de seguridad en los términos del artículo 33 del RGPD. El incidente se gestionó como un incidente en el servicio, en tanto su disponibilidad pudo quedar afectada, trasladando informe técnico a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales conforme al Art. 22 de la Orden IET/1090/2014, de 16 de junio, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas"*.

Indican la cronología de los hechos con los hitos más significativos del incidente:

- En fecha 3 de enero de 2024, con la información publicada en internet, se detecta que el origen de la filtración de la contraseña de RIPE estuvo en un PC de un proveedor de ORANGE, fechándola el 4 de septiembre de 2023 por infección por el *stealer RACCOON* (malware diseñado para rastrear y obtener información sensible de un PC).

- El 4 de enero de 2024 se obtiene información sobre la filtración y se comienza investigación interna, se descarta que ninguna otra credencial comprometida hubiera podido ser utilizada de forma fraudulenta. En esta misma fecha se localiza el PC que había sido afectado.

- El 8 de enero de 2024 ORANGE encarga informe forense del PC a la empresa especializada ZEROLYNX.

- El 18 de enero de 2024 ORANGE recibe el informe forense, este confirma la infección del PC el 4 de septiembre de 2023, detectándose

que el malware accedió a la información contenida en la carpeta *"***CARPETA.1"* donde estaba la información sobre la caché de contraseñas de los navegadores, afirman que no se encontraron evidencias de acceso a información fuera de esa carpeta.

Afirman que, según el informe forense, el malware accedió a la información del PC:

(…).

Indican que:

"*El análisis forense realizado llega a la conclusión de que el usuario del equipo descargó el 4 de septiembre de 2023 a las 10:12:20 un archivo con nombre "KMSPICO.rar" que contenía un malware de tipo Stealer. A las 10:12:59 lo descomprimió y ejecutó. La aplicación maliciosa habría recopilado diferente información del usuario accediendo a la ruta "***RUTA.1" donde se almacena la información de los perfiles de navegación web del usuario, incluyendo la caché de credenciales almacenadas en los navegadores. No existe evidencia de acceso por parte del malware a otras carpetas del equipo. Se han encontrado indicios de que el malware fue parado por Windows Defender y puesto en cuarentena a las 10:14:29.****"***

El Inspector de datos concluye que no existen otras evidencias de posible afectación de datos personales, por lo que el incidente de seguridad no se puede considerar como brecha de seguridad.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con [Introduzca el texto correspondiente a [Texto fundamento I EI].] y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Conclusión

Ha quedado constatado que ORANGE sufrió un incidente de seguridad, en fecha 4 de septiembre de 2023, originado por la entrada del malware RACCON (código malicioso que busca recolectar y exfiltrar información almacenada en el

equipo) en uno de los PC de uno de sus proveedores. Por afirmación de la empresa, se constata que este malware logró acceder a varios ficheros de la carpeta *AppData* donde se almacenaba la caché de contraseñas de los navegadores, filtrándose varias credenciales de ORANGE de aplicativos de carácter técnico, que contenían información sobre despliegues, replanteos, infraestructura de red, etc. sin que a través de ellas se hubiera podido tener acceso a datos de carácter personal.

Dado que no ha quedado acreditado que el incidente de seguridad sufrido por Orange haya supuesto una brecha de datos personales, no se han producido hechos que entren en el ámbito competencial de la Agencia Española de Protección de Datos.

De conformidad con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **ORANGE ESPAGNE, S.A.U.**

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-301023

Mar España Martí
Directora de la Agencia Española de Protección de Datos