- **Procedimiento N.º: E/08750/2020**

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por el responsable del Tratamiento de VODAFONE ESPAÑA, S.A.U. (en adelante VDF o Vodafone) en el que informan a la Agencia Española de Protección de Datos, de accesos indebidos al área de clientes del responsable.

Resumen de la notificación:

Un ataque causó 58.630 intentos de acceso contra MyVodafone app (versión para móviles de MyVodafone) usando la API del backend (interfaz de programación de la aplicación). Tras analizar los intentos de acceso se comprobó que el tráfico consistía en solicitudes de combinación de nombre de usuario y contraseña, usando la API del backend para validar si las credenciales existían en la plataforma de MyVodafone.

Como resultado de este ataque, 277 intentos fueron exitosos por el atacante para 259 clientes. Se detectaron descargas de 185 facturas relacionadas con 171 clientes de entre los 259 afectados.

El atacante utilizó un elevado número (9.980) de direcciones IP diferentes para eludir los controles de seguridad.

Fecha y hora del incidente: ******FECHA.1*** entre las 19:00 y las 21:00.

Categoría de datos afectados:

Credenciales de acceso o identificación y datos de factura:

- Usuario y contraseña de 259 clientes.
- Datos de factura de 171 clientes (nombre, apellidos, dirección, DNI, líneas contratadas, tarifa, últimos 4 dígitos de la cuenta bancaria).

SEGUNDO: En fecha 26 de octubre de 2020, la Directora de la Agencia Española de Protección de Datos ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: ******FECHA.2***.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:
VODAFONE ESPAÑA, S.A.U. (VDF)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fecha 21/12/2020 se solicitó información a VDF. De la respuesta recibida se desprende lo siguiente:

El ******FECHA.1***, la aplicación de Mi Vodafone experimentó un ataque de *credential stuffing* (ataque utilizando credenciales de los usuarios obtenidas de forma previa). Esta actividad fue detectada como resultado del alto volumen de intentos de acceso usando la API del backend bajo múltiples direcciones IP con un alto ratio de número de intentos erróneos.

Los análisis de VDF concluyen que el atacante utilizo métodos que le permitieron realizar intentos legítimos de acceso, para validar si algunas de las credenciales existían en la plataforma.

Manifiestan que, de estos intentos, tienen constancia de que 259 cuentas le devolvieron un resultado satisfactorio al atacante. Las contraseñas de las cuentas afectadas fueron reseteadas y se implementaron contramedidas, indicadas más adelante. Los representantes de VDF indican que estas medidas anularon por completo la efectividad del ataque.

En concreto, con respecto al carácter de la brecha y el origen de las credenciales utilizadas en el ataque VDF ha manifestado:

> *"El pasado día *****FECHA.1** se detectó una actividad inusual en los accesos a Mi Vodafone App haciendo uso no legítimo de la API que permite el logado en la aplicación móvil, simulando el acceso producido por un móvil con iOS y la aplicación Mi Vodafone.*
>
> *Esta actividad consistió en un alto volumen de intentos de acceso (58630) mediante el uso de conjuntos de credenciales de usuario y contraseña con un origen externo a Vodafone España.*
>
> *El análisis realizado determinó que el tráfico eran solicitudes de combinación de nombre de usuario y contraseña (Credential Stuffing) que estaban usando la API del backend para validar si las credenciales existían en la plataforma de Mi Vodafone.*
>
> *Un porcentaje de las credenciales intentadas, produjeron una validación correcta, por la razón de que algunos usuarios utilizan el mismo conjunto de credenciales en distintos portales online. Este hecho permitió al atacante la validación positiva (login correcto) de 259 cuentas de Mi Vodafone.*
>
> *El atacante utilizó un elevado número de IPs (9.980) diferentes para eludir los controles de seguridad.*

El método empleado por el atacante consiste en, haciendo uso de múltiples IPs de origen y de conjuntos de credenciales extraídas de internet, realizar un intento de usuario y contraseña por cada registro contra Mi Vodafone."

Adjuntan el fichero Excel con todas las cuentas empleadas por el atacante, verificándose que consta 58629 registros (el número 1 es una cabecera).

Respecto al porcentaje de intentos de acceso fallidos VDF ha manifestado:

"Durante la franja horaria del ******FECHA.1****, entre las 19:00pm y las 21:00pm, Vodafone detectó un incremento de KOs en la monitorización de la API de logado de Mi Vodafone App, en donde se llegó a generar una tasa de accesos fallidos en torno al 99%.*

Derivado de esta alarma, Vodafone identificó que había múltiples IPs extranjeras que estaban realizando intentos de acceso a Mi Vodafone, empleando la backend API para realizar intentos de login. "

Indican que en el fichero Excel que adjuntan se muestra *"toda la actividad producida por el atacante en Mi Vodafone App, durante la franja horaria indicada anteriormente. En base a esta actividad, y con el conocimiento de los equipos técnicos de Vodafone, se identificaron aquellos accesos susceptibles de ser fraudulentos, dado que el atacante empleaba en su ataque una versión de la app de iOS (6.8.3) que ya no estaba oficialmente permitida su uso dado que entre el 8-9 de octubre, se realizó un forceupdate a todos los usuarios obligando a tener la versión 6.8.10 de la app para poder seguir haciendo uso de ella."*

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

Se ha requerido a VDF para que aporte el detalle de las medidas de seguridad implementadas con anterioridad a la brecha aplicables a la misma (para evitar accesos no autorizados a la app) e información sobre si se han modificado dichas medidas con posterioridad a los hechos. Se pide detalle de la política de contraseñas para el acceso a la aplicación implementada. Se tiene constancia por la brecha de 08/02/2020 y 07/04/2020 de la implementación adicional de diversas medidas como el CAPTCHA. Se les pide información detallada sobre las medidas adicionales adoptadas entre la ocurrencia de las citadas brechas y la presente. Los representantes de VDF han manifestado que:

"A raíz de los incidentes notificados en fecha 08/02/2020 y 07/04/2020 que consistieron en una continuación del mismo ataque, se reforzaron las medidas de seguridad implementadas en Mi Vodafone App, de la siguiente forma:

- *Módulo de credential stuffing de […] con implementación en el WAF.*
- *Implementación de una protección basada en Captcha de Google V2.*
  Esta versión valida los intentos de acceso no se produzcan por un robot / intentos automatizados, sin embargo, no realiza una evaluación precisa sobre la reputación de las IP de origen.

Por ello, tras los intentos de acceso reportados en la comunicación adicional el 07 de abril de 2020, se implementó como mejora a las medidas de seguridad ya indicadas una nueva versión de Captcha, el Captcha V3 de Google. Con esta versión, además de incorporar los mecanismos de seguridad de la V2, con la misma nos aseguramos de que aquellas IP que tengan mala reputación cuenten con mayores barreras de seguridad para lograr el acceso y se evita el uso de scripts para automatizar la resolución del Captcha.

- *Comienzo del desarrollo de una solución de doble factor de autenticación para el login de AppWeb Mi Vodafone.*
- *Incremento de las reglas de monitorización y alertas implementadas.*
- *Revisión de las mejoras que pueden hacerse para monitorizar la reputación de las IP.*
- *Nueva regla para los inicios de sesión fallidos por IP, se detectan más de […] solicitudes de fallo en un minuto con un tiempo de espera de […].*
- *Implementación de un sistema de doble factor de autentificación (2FA) dentro de MiVodafone para poder efectuar la contratación de servicios de valor añadido (como Netflix).*

Se debe tener en cuenta que las medidas implementadas en las anteriores brechas, el atacante hizo uso de las versiones Web de Mi Vodafone. Por este motivo, no todas las medidas de seguridad implementadas a raíz de dichas incidencias aplican a la presente brecha de seguridad dado que la misma se ha producido usando el entorno de la App de Mi Vodafone para dispositivos móviles y no la versión WEB de la Mi Vodafone."

Respecto de las medidas implementadas con posterioridad la brecha

Los representantes de VDF declaran que *"Tras la notificación de la brecha de seguridad el día 19/10/2020, se han mejorado las medidas de seguridad anteriores"* VFN indica 6 medidas concretas relacionadas con la API, contraseñas, monitorización, y reglas del WAF.

Indican que se ha enviado un SMS a los afectados informándoles sobre la necesidad de realizar un reseteo de la contraseña para acceder a Mi Vodafone. (16 de octubre) así como que el desarrollo del doble factor de autenticación para iniciar sesión en Mi Vodafone, tanto en web como en App, sigue en desarrollo. Actualmente ya se encuentra en fase final de pruebas y se prevé que la misma sea publicada a finales del mes de enero 2021.

Aportan también la política de contraseñas para la aplicación implementada.

Respecto de las medidas de minimización del impacto de la brecha

Los representantes de VFD manifiestan:

- Se restringe el acceso, de forma temporal, a Mi Vodafone mediante geolocalización. (******FECHA.1***)

- Se ha realizado un restablecimiento de las contraseñas en las cuentas de los clientes identificados como parte de la contención. (3:00 AM hora local 16 de octubre).
- Se ha enviado un SMS a los afectados informándoles sobre la necesidad de realizar un reseteo de la contraseña para acceder a Mi Vodafone. (16 de octubre).
- Se lanza la app rediseñada de Mi Vodafone versión 6.11.3 iOS, 6.11.1 Android (3 de noviembre y 31 de octubre respectivamente)

Respecto de los datos afectados.

Tipología de los datos accedidos. Credenciales de acceso a Mi Vodafone de un total de 259 clientes.

De entre esos 259 clientes, se ha detectado que el atacante descargó facturas de 171 clientes que han sido identificados internamente con el fin de monitorizar su actividad y poder marcarlos como potenciales víctimas de fraude, así como informados específicamente del posible acceso a sus datos.

Los datos que aparecen en una factura son los siguientes: nombre, apellidos, dirección, DNI, líneas contratadas, tarifa, últimos 4 dígitos de la cuenta bancaria).

Número final de afectados detectados: 259

Respecto de la notificación remitida a los afectados:

Los representantes de VDF han declarado haber realizado varias notificaciones a los afectados.

Indican que se llevó a cabo el envío de una comunicación a todos los usuarios afectados, a través de un SMS, informando sobre la necesidad de restablecer sus contraseñas el día 16 de octubre.

El texto aportado por VDF del SMS es el siguiente:

> *"VF Info: Hemos detectado intentos de acceso sospechosos en tu cuenta de Mi Vodafone. Para tu seguridad, hemos reseteado tu contraseña. Entra en Mi Vodafone para establecer una nueva distinta a la anterior. Te recomendamos revises otras cuentas que protejas con las mismas credenciales."*

El día 20 de octubre se enviaron notificaciones con la información completa a los usuarios afectados informando del alcance de la brecha de seguridad.

Estas notificaciones se enviaron a través de la App Mi Vodafone y se diferenciaron por el tipo de datos comprometidos (credenciales de acceso o datos incluidos en facturas).

De este modo, la notificación remitida a aquellos 171 usuarios de los que se descargaron facturas es la siguiente:

"Con anterioridad te informamos por SMS de que habíamos detectado accesos no autorizados a Mi Vodafone. Creemos que esto se debe a que usas el mismo usuario y contraseña para acceder a otras webs. El usuario y contraseña de Mi Vodafone no se obtuvieron de Vodafone. Te recomendamos que cambies estas credenciales en todos las webs y apps en donde las utilices.
Como precaución se bloqueó tu cuenta de Mi Vodafone y se reestableció la contraseña, por lo que te pedimos que elijas una nueva contraseña que no uses en otros sitios online. Puedes cambiar tu contraseña en el apartado Datos de acceso a Mi Vodafone de la sección Tu Cuenta. Como consecuencia del acceso, es posible que tus datos, incluidos los datos de facturación, se hayan visto comprometidos. En Vodafone nos tomamos la seguridad muy en serio y podemos asegurar que hemos tomado medidas de manera inmediata para proteger su información y seguiremos vigilando cualquier actividad inusual para garantizar su seguridad.
Esto ha sido notificado a la Agencia Española de Protección de Datos y se han tomado las medidas oportunas para preservar tu seguridad y privacidad en Mi Vodafone.
Vodafone vela por la seguridad y cuenta con un equipo internacional de profesionales de ciberseguridad que continuamente monitorizan, protegen y defienden nuestras redes. Para más información puedes contactarnos en ******EMAIL.1****".*

Mientras que a los restantes 88 usuarios de los que se comprometió la información de sus credenciales de acceso se les remitió la siguiente comunicación en la que se matiza el tipo de datos comprometidos:

"Con anterioridad te informamos por SMS de que habíamos detectado accesos no autorizados a Mi Vodafone. Creemos que esto se debe a que usas el mismo usuario y contraseña para acceder a otras webs. El usuario y contraseña de Mi Vodafone no se obtuvieron de Vodafone. Te recomendamos que cambies estas credenciales en todos las webs y apps en donde las utilices.
Como precaución se bloqueó tu cuenta de Mi Vodafone y se reestableció la contraseña, por lo que te pedimos que elijas una nueva contraseña que no uses en otros sitios online.
Puedes cambiar tu contraseña en el apartado Datos de acceso a Mi Vodafone de la sección Tu Cuenta. En Vodafone nos tomamos la seguridad muy en serio y podemos asegurar que hemos tomado medidas de manera inmediata para proteger su información y seguiremos vigilando cualquier actividad inusual para garantizar su seguridad.
Esto ha sido notificado a la Agencia Española de Protección de Datos y se han tomado las medidas oportunas para preservar tu seguridad y privacidad en Mi Vodafone.
Vodafone vela por la seguridad y cuenta con un equipo internacional de profesionales de ciberseguridad que continuamente monitorizan, protegen y defienden nuestras redes. Para más información puedes contactarnos en ******EMAIL.1****".*

Utilizaciones posteriores detectadas de los datos accedidos. Posibles consecuencias para los afectados.

Los representantes de VDF han manifestado que en las investigaciones posteriores realizadas por los equipos de monitorización locales y de global no se han detectado actividades anormales en las cuentas de los usuarios afectados ni reclamaciones por parte de estos.

Respecto de las acciones tomadas para la resolución final de la brecha

Los representantes de VDF describen las acciones que ha sido realizadas para la resolución final de la incidencia indicando que consta cerrada a nivel interno:

- Nuevas reglas de monitorización del WAF (noviembre).
- Se lanza la app rediseñada de Mi Vodafone versión 6.11.3 iOS, 6.11.1 Android (3 de noviembre y 31 de octubre respectivamente).
- Se fuerza la actualización a los usuarios para las nuevas versiones de iOS y Android (4 noviembre).
- Análisis de hacking ético en la app (11 noviembre).
- Sigue en desarrollo el 2FA para logado en Mi Vodafone. Actualmente en fase final de pruebas y se prevé que la misma sea publicada a finales del mes de enero 2021.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 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.

II

El artículo 4 del RGPD, en su apartado 12, establece que a efectos del presente Reglamento se entenderá por *«violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."*

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, como consecuencia de un ataque de credential stuffing (ataque utilizando credenciales de los usuarios obtenidas de forma previa). Esta actividad fue detectada como resultado del alto volumen de intentos de acceso bajo múltiples direcciones IP con un alto ratio de número de intentos erróneos.

En el presente caso, tras el requerimiento de información llevado a cabo por la inspección de esta AEPD, la entidad investigada ha informado de las investigaciones internas realizadas y del resultado de estas.

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en

función de los posibles riesgos estimados, pero, sin embargo, se produjo la incidencia ahora analizada. Se debe tener en cuenta que las medidas implementadas en las anteriores brechas de fecha 8 de febrero de 2020 y 7 de abril de 2020, el atacante hizo uso de las versiones Web de Mi Vodafone. Por este motivo, no todas las medidas de seguridad implementadas a raíz de dichas incidencias se aplican a la presente brecha de seguridad, dado que la misma se ha producido usando el entorno de la App de Mi Vodafone para dispositivos móviles y no la versión WEB de MiVodafone.

Asimismo, contaba con protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

Se debe destacar la rápida actuación de la entidad desde el mismo momento en que tuvo conocimiento de los hechos, interviniendo de forma activa en su resolución, minimizando los posibles efectos perniciosos del incidente, toda vez que las contraseñas de las cuentas afectadas fueron reseteadas y se implementaron contramedidas que anularon por completo la efectividad del ataque.

No constan reclamaciones ante esta Agencia por parte de terceros.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente, mejorando las medidas de seguridad. Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

III

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de la entidad investigada como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo 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 VODAFONE ESPAÑA, 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.

940-0419

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