Fuga de información de AEDyR

Visión del analista

El 7 de abril de 2016, se produjo una brecha de seguridad en la Asociación Española de Desalación y Reutilización. Debido a un ataque de *SQL injection* en su página web fue extraída información acerca de socios y empresas pertenecientes a AEDyR. La lista de afectados es bastante extensa e incluye empresas de diferentes sectores relacionadas con el tratamiento de aguas e infraestructuras. Entre la información filtrada se encuentran multitud de credenciales corporativas de personas relacionadas con estos sectores.

La filtración de credenciales es una amenaza para la seguridad corporativa, incluso aunque estas se produzcan en activos tecnológicos de terceros. Desde el servicio de CyberThreats no se ha localizado ningún tipo de notificación por parte de AEDyR ni en su página web oficial ni en los medios sociales corporativos. Tampoco se han encontrado noticias relacionadas acerca de la fuga de datos, por lo que no podemos determinar si los afectados han sido informados sobre el incidente.

Ficha técnica

Objetivo del ataque:	**AEDyR**
Sector:	**Tratamiento de agua**
Fecha del ataque:	**07/04/2016**
Motivación:	**Cibercrimen**
Autoría:	**Pyopz**
Activos afectados:	**Base de datos de usuarios**
Naturaleza de la información filtrada:	**Datos personales, DNI, Teléfono, Email, Contraseña**
Volumen de información:	**715 Registros**
Disponibilidad en línea:	**SÍ** (17 de mayo de 2016)

AEDyR
ASOCIACIÓN ESPAÑOLA DE DESALACIÓN y REUTILIZACIÓN

Presencia de la compañía:

España

Detalles de la filtración

Origen de las credenciales

La filtración de datos se hizo pública el día 8 de abril en una plataforma web dedicada a la compartición de filtraciones en formato texto. Tras ser liberada la información, el autor de la fuga se puso en contacto a través de Twitter[1] con diferentes páginas web dedicadas a identificar y catalogar este tipo de brechas de seguridad.

El enlace contenía credenciales agrupadas en dos apartados diferentes. La primera parte del contenido era una tabla con 305 registros, que contenían los siguientes campos: dirección, nombre, apellidos, teléfono, email, localidad, fax, nombre de la compañía, DNI, CIF, fecha de alta y contraseña. Esta última se almacenaba usando un algoritmo de *hashing* MD5 de 128 bits. La segunda parte contenía otra tabla con 410 registros que incluían teléfono, cuenta de correo y código postal.

En total, se identificaron 417 cuentas de correo electrónico afectadas, las cuales estaban repartidas en más de 180 dominios diferentes, siendo en su mayoría de carácter corporativo. En al menos 20 empresas se exponía la totalidad de sus credenciales, por lo que la posible suplantación de las identidades registradas es elevada. Como se puede ver en la Tabla 1, una parte significativa pertenecen a dominios *.es* debido al ámbito nacional de la compañía.

Dominios más afectados	Número de
Empresa_Infraestructuras_1	12
Empresa_Tratamiento_Aguas_1	11
gmail.com	10
Empresa_Tratamiento_Aguas_2	10
Empresa_Tratamiento_Aguas_3	10
Universidad_1	8
Empresa_Tratamiento_Aguas_4	7
Empresa_Química_1	6
Empresa_Infraestructuras_2	6
Empresa_Infraestructuras_3	5
Empresa_Tratamiento_Aguas_5	5
Empresa_Infraestructuras_4	5
Empresa_Infraestructuras_5	5
Empresa_Tratamiento_Aguas_6	5
yahoo.es	5

Distribución por tipo de dominio

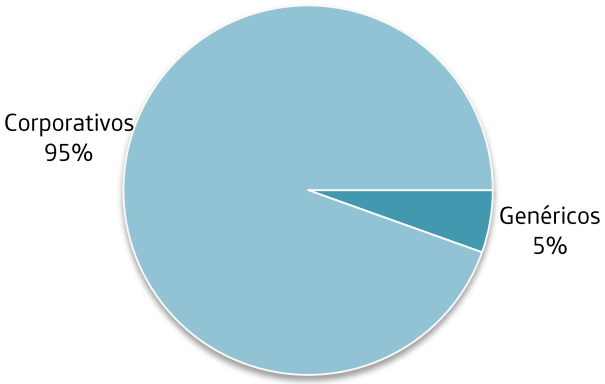

Tabla 1. Distribución de dominios y cuentas de correo afectadas.

Presuntos responsables

El presunto autor de la filtración se identifica con una cuenta de Twitter bajo el alias de @pyopzi que ya ha sido eliminada de la red social. Posteriormente, se pudieron identificar otras identidades que posiblemente estaban relacionadas como @pyopzed[2] o @pyopzidsadas[3].

1 @pyopz, "Pyopz", Twitter. [En línea]. Disponible en: https://twitter.com/pyopz/. [Accedido: 12-may-2016].

2 @pyopzed, "Pyopz☀", Twitter. [En línea]. Disponible en: https://twitter.com/pyopzed. [Accedido: 12-may-2016].

3 @pyopzidsadas, "Pyopz", Twitter. [En línea]. Disponible en: https://twitter.com/pyopzidsadas. [Accedido: 12-may-2016].

La cuenta de @pyopzidsadas que se describe como «Investigador de seguridad» y «*Hacktivista*», se encontró una mención explícita a una plataforma[4] de publicación de fugas de información. En el fichero aparece un nuevo usuario bajo el alias de @pyopz, en cuyo perfil de Twitter se recogen *tweets* con fecha 5 de abril en los que intenta ponerse en contacto con algunas páginas web vulnerables. Tras no recibir respuesta, las expuso el día 7.

Asimismo, el presunto autor había estado colaborando con el grupo *hacktivista* Anonymous en la operación #OpBeast encargada de la identificación y eliminación de páginas dedicadas al abuso sexual de animales. Posteriormente se confirmó como un nuevo pseudónimo creado a partir de la cuenta de @pyopzed, donde su perfil ya se describe como «Hacker de sombrero negro». Este último alias encontrado (@pyopz) tenía publicado un enlace a otro fichero en la misma plataforma anteriormente mencionada, que contenía un listado adicional de direcciones web y en el que indica explícitamente la posibilidad de comprar otras filtraciones que todavía no han sido publicadas. Entre los archivos encontrados en la lista, estaba la filtración de AEDyR, además de la divulgación de las credenciales pertenecientes a siete páginas web, que también habían sido vulneradas por el mismo autor. En dos de las últimas filtraciones, a parte de las cuentas de Twitter, menciona como vía de contacto una cuenta de correo cifrado[5].

El día 9 de abril, anuncia en el perfil de @pyopzidsadas, un último cambio de cuenta en la plataforma de Twitter bajo el nuevo alias de @pyopze donde recomienda a la comunidad *hacker* no realizar actividades delictivas. Desde el día 10 de abril cesó toda comunicación.

En la Figura 1, se adjunta una captura del análisis realizado, donde se puede observar como punto de partida la dirección web donde fue publicada, hasta localizar el fichero donde se encontraban almacenadas originalmente las credenciales filtradas.

Posibles usos y recomendaciones generales

Los activos tecnológicos de terceros son objetivos atractivos para los delincuentes ya que incluso los entornos corporativos mejor protegidos van a ver cómo sus usuarios interactúan con otras plataformas que no necesariamente han de cumplir con los estándares de seguridad deseados. En cualquier caso, este tipo de anuncios ponen sobre la mesa dos formas criminales relevantes. Por un lado, la figura del delincuente que ha logrado un acceso ilícito a una plataforma y que puede comerciar con la información filtrada. Por otro, la existencia de cuentas de correo electrónico corporativas y la naturaleza misma de la filtración que, al estar orientada al mercado laboral, convierten a los perfiles expuestos en objetivos de ataques dirigidos con mayores probabilidades de éxito con el contexto adecuado. En este sentido, una mala práctica a la hora de gestionar las contraseñas de los usuarios podría suponer una ventana de oportunidad para los atacantes que podrían lograr acceso a algunas cuentas si consiguen romper los *hashes* de las contraseñas almacenadas.

4 About - Ghostbin. [En línea]. Disponible en: https://ghostbin.com/about. [Accedido: 11-may-2016].

5 Los emails seguros convertidos en una brisa, Tutanota. [En línea]. Disponible en: https://tutanota.com/es. [Accedido: 12-may-2016].

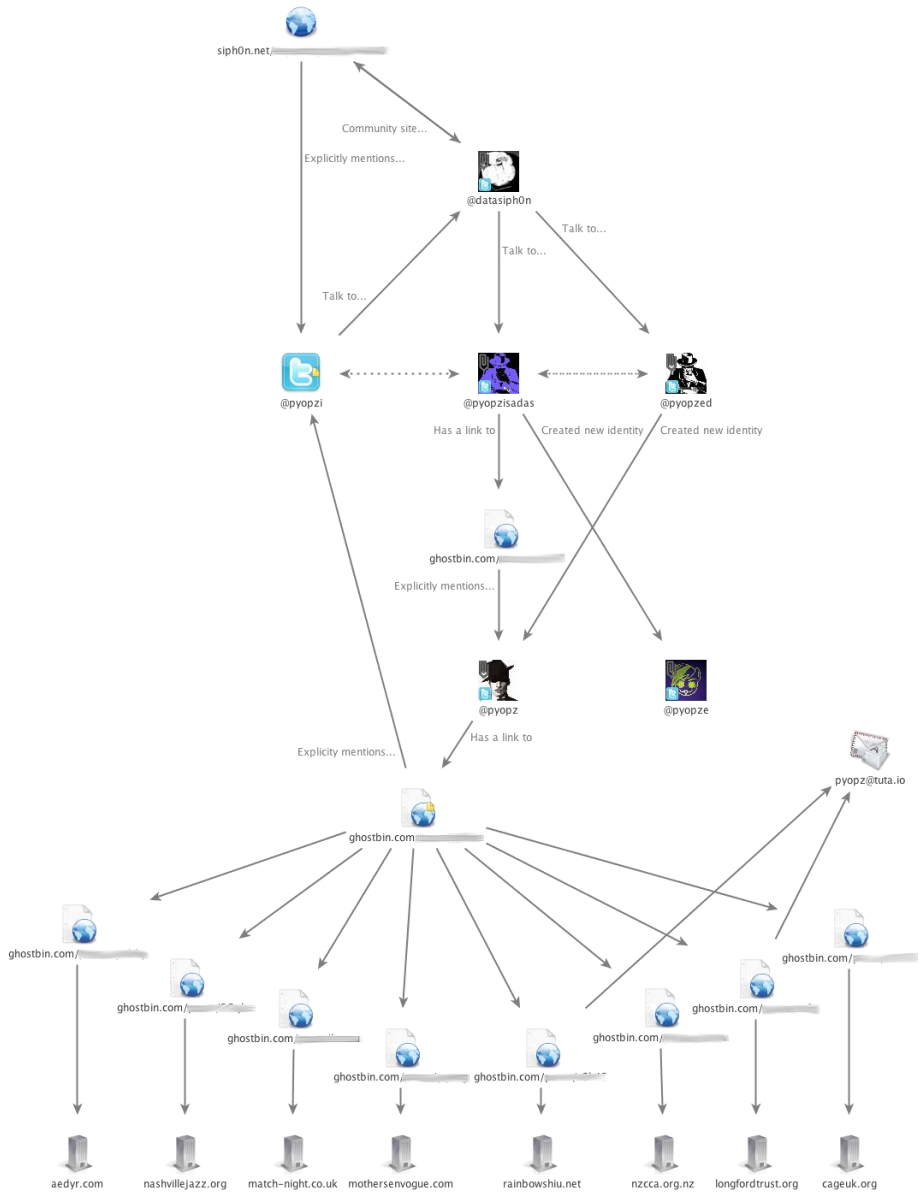

Figura 1. Relación de la información identificada a partir de la dirección que contenía las credenciales robadas.