Operación “Oil Tanker”

La Amenaza Fantasma

Operación Oil Tanker: La Amenaza Fantasma.

Todo comenzó un frío día de enero en una ciudad costera del noreste de Inglaterra. Un lugar con una prominente industria petroquímica, con todo tipo de empresas del sector.

En una de estas empresas el día comenzó de forma normal, se trata de una compañía que se encarga, entre otras cosas, del transporte marítimo de petróleo. Llamaremos a esta compañía “Black Gold”.

John, el responsable de seguridad informática de Black Gold sabe que vivimos en un mundo peligroso, que los ataques de malware están a la orden del día. Si bien Black Gold no está en la lista del Fortune 1000, él sabe que todas las precauciones son pocas y que si bien una solución antivirus es imprescindible, hay que maximizar todas las medidas de seguridad en una empresa como la suya.

Es por ello que cuando le ofrecieron participar en un piloto de un nuevo servicio que monitorizaba las ejecuciones en los endpoints y le aportaba información del estado de seguridad de su parque, así como datos forenses en caso de producirse un incidente, no se lo pensó. Tras una serie de pruebas controladas, decidió desplegar el pequeño agente a toda su red en octubre.

Durante los tres primeros meses la información recibida le ayudó a identificar equipos que estaban en riesgo por ejecutar aplicaciones vulnerables, pero aparte de eso no había sucedido nada reseñable.

Gracias a John, Black Gold entró a formar parte de un piloto de alta seguridad informática.

panda

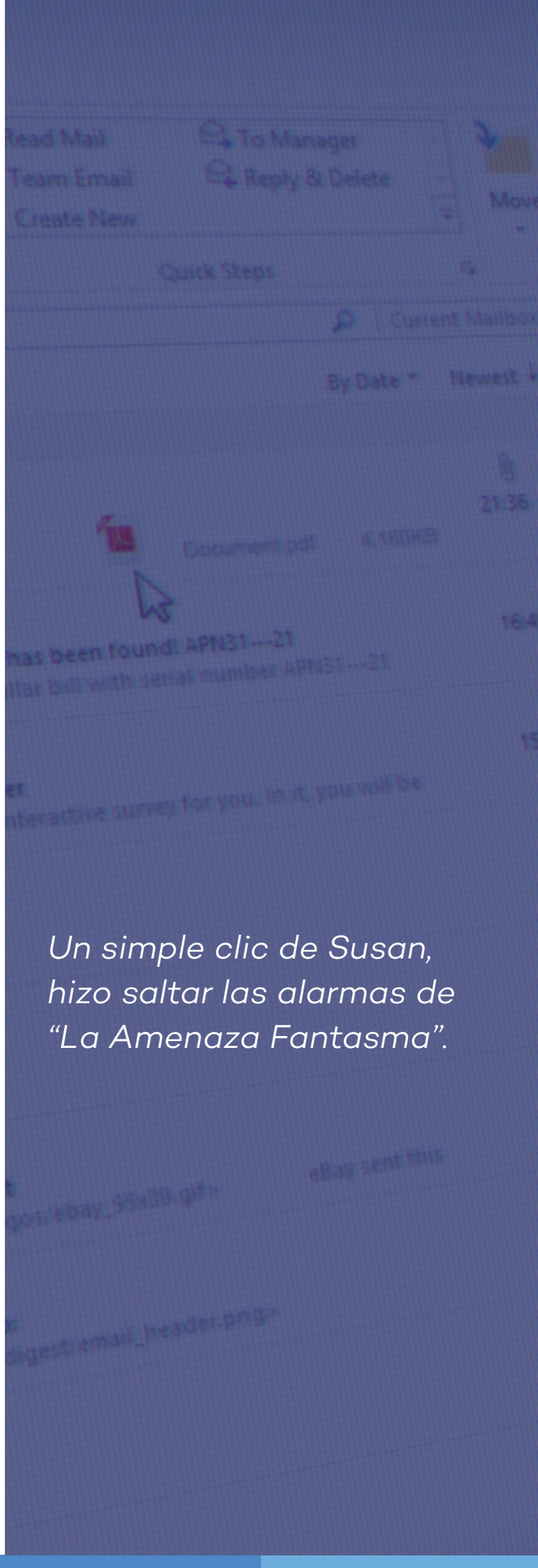
Susan, que lleva más de 20 años trabajando como secretaria en Black Gold, estaba revisando el correo electrónico que, como cada lunes se acumulaban en la bandeja de entrada, cuando llegó a un correo con un documento adjunto.

Aparentemente se trataba de un fichero PDF de unos 4Mb de tamaño con información sobre el mercado petrolífero, nada sospechoso. Además había pasado todos los filtros de seguridad. Ni el antivirus del servidor de correo, ni el de su equipo de trabajo, habían detectado ningún tipo de amenaza.

Tras hacer doble clic en el fichero, se abrió un PDF pero estaba en blanco. "Se han equivocado al adjuntar el fichero, ya se darán cuenta y lo volverán a enviar", pensó Susan mientras continuó con los siguientes mensajes que tenía pendientes.

Al mismo tiempo, a 1.700km de distancia, una alerta comenzó a sonar. Una amenaza desconocida acababa de ser bloqueada cuando trataba de robar credenciales del ordenador de Susan y enviarlas al exterior.

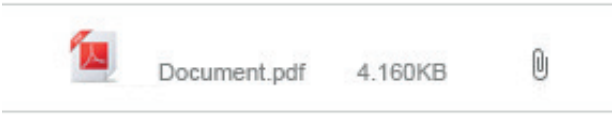
Hoy en día la mayoría de las amenazas tratan de robar información de sus víctimas, así que este caso parecía uno de los miles que cada día analizamos. Nos llamó la atención que ningún motor antivirus era capaz de detectar el fichero, aunque si tenemos en cuenta que cada día aparecen más de 250.000 nuevas muestras de malware tampoco es algo tan raro. Sin embargo, había algo que lo hacía diferente: no utilizaba malware. Esto hizo que internamente denomináramos el ataque como "La Amenaza Fantasma".



Un simple clic de Susan, hizo saltar las alarmas de "La Amenaza Fantasma".

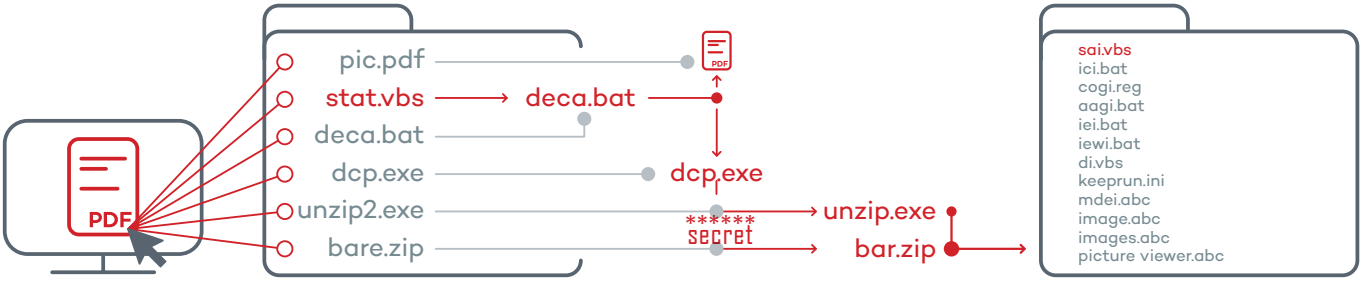
Análisis del ataque

El fichero que Susan vio en su correo y abrió a continuación tenía este aspecto.



Realmente se trataba de un fichero ejecutable que utilizaba el icono de documentos de Adobe Acrobat Reader para engañar a la víctima.

En la siguiente figura podemos observar el flujo de ejecución:



El fichero se trataba simplemente de un autodescomprimible. Una vez ejecutado lo único que hace es crear una carpeta donde descomprime seis ficheros, ejecuta uno de ellos –stat.vbs- y finaliza.

Ningún comportamiento malicioso que pudiera hacer saltar la alarma de un análisis de comportamiento de la aplicación.

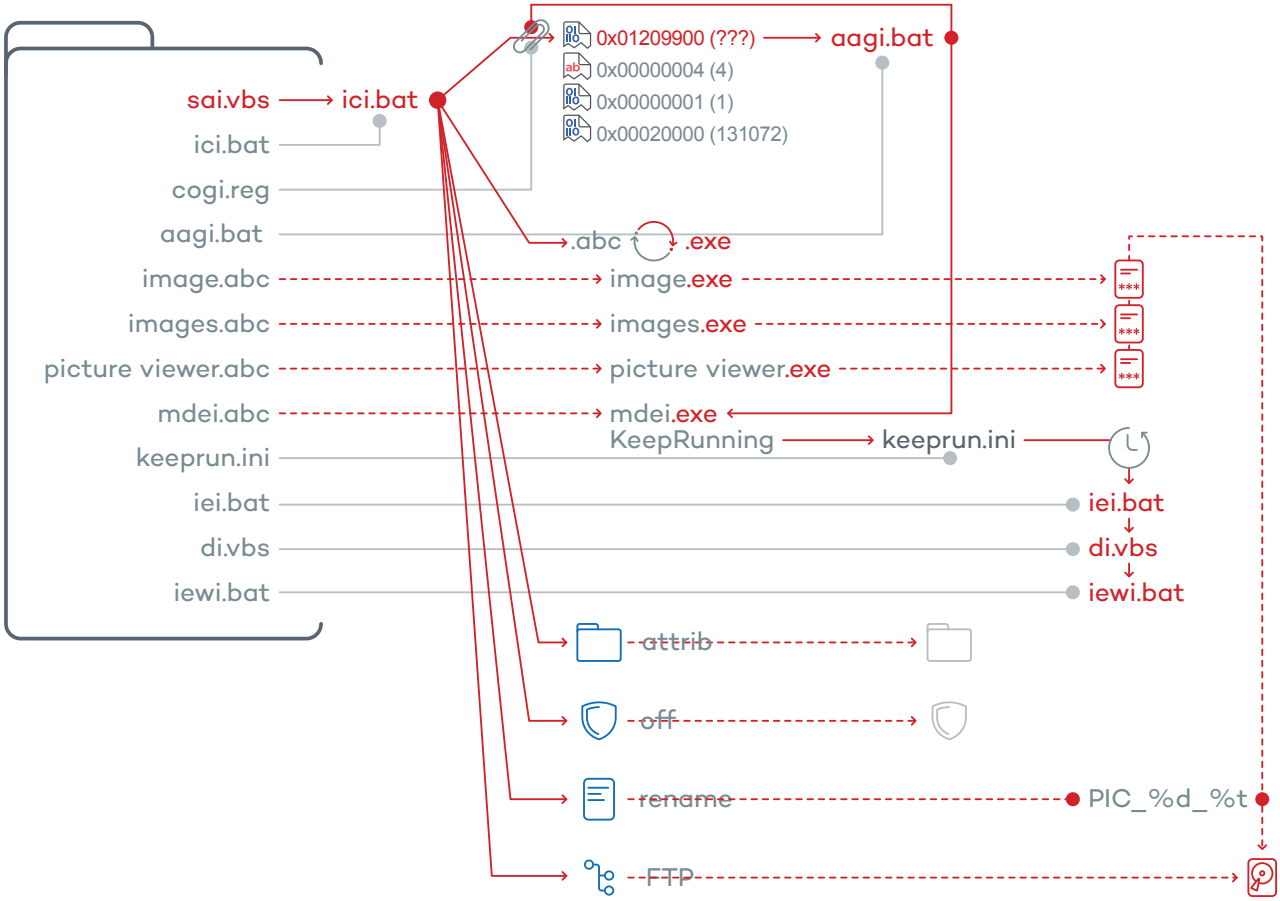
El fichero vbs ejecutado simplemente ejecuta un segundo fichero llamado deca.bat. Éste se encarga de abrir el fichero pic.pdf (el documento pdf que Susan vio abrirse en su ordenador y que está vacío).

A continuación ejecuta el fichero dcp.exe, una herramienta gratuita que permite cifrar ficheros. Lo utiliza para descifrar los dos ficheros restantes:

unzip2.exe ⟶ unzip.exe
bare.zip ⟶ bar.zip

Una vez hecho esto utiliza el programa unzip.exe para descomprimir en otra carpeta el contenido de bare.zip, un total de 12 ficheros. Tras este paso, ejecuta uno de estos ficheros, el sai.vbs.

Sigue sin producirse ningún comportamiento anómalo ni nada parecido a lo que vemos a diario en todo tipo de ataques. Aquí se inicia la siguiente parte del ataque:



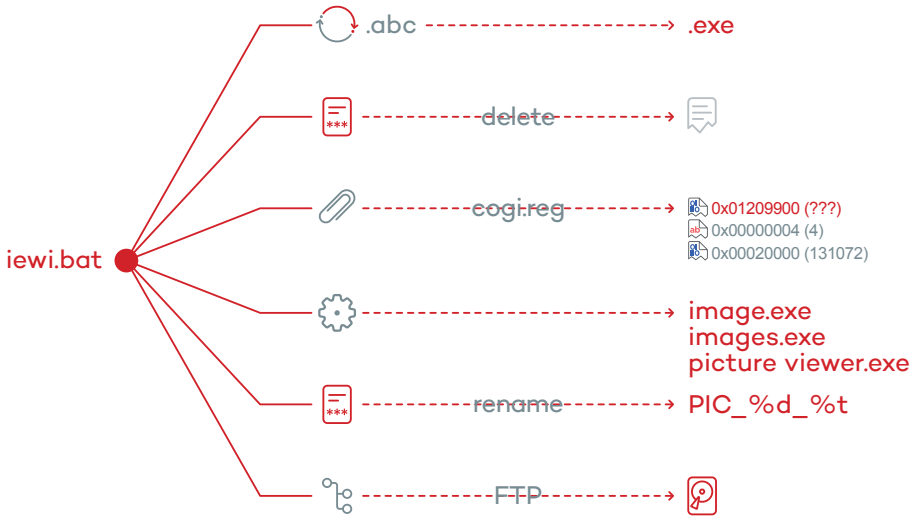
El vbs ejecuta un fichero bat que modifica el registro de Windows para que cada vez que se inicie el sistema se ejecute el fichero aagi.bat. A continuación hace una copia de los cuatro fichero que tienen extensión abc y cambia su extensión a .exe. Se trata de aplicaciones legales que cualquier usuario en un momento dado podría utilizar: las tres primeras son herramientas que toma todas las credenciales (nombres de usuario y contraseñas) que tenemos salvadas tanto en nuestro cliente de correo local como en el navegador y las vuelca a un fichero de texto.

La cuarta se trata de una aplicación que se encarga de ejecutar una aplicación cada “x” tiempo, muy útil por ejemplo en terminales que tienen que estar siempre ejecutando una aplicación, como un navegador o cualquier otro tipo de software, de tal forma que si por algún problema se cierra de forma imprevista esta aplicación la vuelve a abrir. En este caso está configurado para ejecutar otro fichero bat cada 3.600 segundos (una hora).

A continuación se utiliza el comando del sistema attrib para marcar como ocultas las dos carpetas creadas, desactiva el firewall de Windows y renombra los ficheros de texto que contienen las credenciales al formato PIC_%d_%t. El %d se trata de la fecha y el %t de la hora actual, de esta forma se puede saber en qué momento se ha obtenido la información que contienen.

Por último utiliza el comando ftp para subir estos ficheros a un ftp externo controlado por los atacantes.

Finalmente, cada hora se ejecuta el fichero iei.bat, que básicamente realiza lo siguiente:



Vuelve a copiar los ficheros .abc a .exe, por si hubieran sido eliminados. Borra los ficheros de texto con credenciales que han sido ya subidos al ftp, vuelve a introducir la entrada de registro de Windows por si hubiera sido eliminada, ejecuta las aplicaciones que extraen las credenciales, renombra los ficheros resultantes y los sube de nuevo al ftp.

Como se puede observar, en ningún caso se ha utilizado malware como tal, todo el ataque se basa en la utilización de herramientas legales y varios scripts que llevan a cabo las acciones descritas.

¿Es este un tipo de ataque efectivo? Como comentábamos anteriormente, ningún antivirus aparentemente era capaz de detectar este ataque, y las peculiaridades de su comportamiento en ejecución hacían prever que otras capas de protección proactivas incluidas en la mayoría de soluciones antivirus no se activarían ante lo aparentemente inocuo de la mayoría de sus acciones.

Esto se confirmó cuando logramos acceder al servidor ftp donde se enviaban los datos robados y vimos que los primeros eran de agosto del año anterior, el ataque llevaba en marcha casi medio año sin que nadie se hubiera dado cuenta.

¿Ataque dirigido?

Cuando logramos acceder al ftp, en primer lugar hicimos una búsqueda de credenciales de Black Gold, ya que si bien habíamos parado el ataque en el ordenador de Susan podría darse el caso de que otro empleado hubiera sido víctima del mismo ataque. El resultado fue negativo, no habían robado credenciales de la empresa.

Nos sorprendió la cantidad de ficheros que había en el ftp, más de 80.000 ficheros de texto con credenciales robadas. Claramente **no parecía un ataque dirigido**, que suele estar circunscrito a un número limitado de víctimas.

Sin embargo, tras abrir tres de estos ficheros al azar, vimos que contenían credenciales de tres empresas que pertenecían al mismo sector. Casualmente el mismo sector al que pertenecía Black Gold.

Como hemos descrito en el apartado anterior, el ataque se ejecutaba de forma recurrente cada hora. Esto significa que cada hora se envían las credenciales robadas al ftp. Eliminamos los ficheros duplicados y nos quedamos con 860 ficheros únicos.

Aún parecían demasiados para poder decir que estábamos ante un ataque dirigido. Ya no quedaba más que procesar manualmente todos estos ficheros y tratar de identificar a sus víctimas.

En total se trataba de una decena de empresas, todas pertenecientes al mismo sector del transporte marítimo de gas y del petróleo.

Quedaba claro que se trataba de un ataque dirigido, pero no sabíamos qué es lo que los atacantes estaban buscando ni cuál era su objetivo final.

Lo que en un principio no parecía ser un ataque dirigido, terminó siendo una trama conspirativa en el sector.

Nigeria, scams y petróleo

Los timos nigerianos son conocidos desde el inicio de los tiempos de Internet, incluso se venían produciendo desde antes a través de correo físico.

El más conocido es el que se hace pasar por alguna figura relevante del gobierno nigeriano o de alguna institución del país, que contacta con nosotros para que le ayudemos a sacar una importante cifra de dinero de su país y a cambio nos dará un porcentaje del dinero que saquemos.

Pero la industria del timo nigeriano es muy amplia, y hay algunos que no son conocidos por el gran público pero que abarcan todo tipo de sectores. Incluyendo el petrolero.

Existe en Nigeria una ciudad llamada Bonny que es muy famosa en el sector petrolero, ya que el petróleo que se extrae de allí, conocido como Bonny Light Crude Oil (BLCO), tiene un contenido de azufre muy bajo, lo que hace que sea codiciado por las refinerías debido a que por su composición produce mucha menos corrosión.

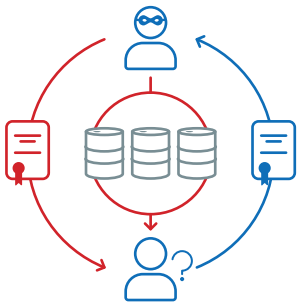
El hecho de que este tipo de petróleo sea tan deseado ha hecho que exista un fraude dirigido a brokers del sector, compradores de crudo que están deseando comprar a buen precio producto de muy buena calidad, siendo el BLCO su máximo exponente.

En Nigeria todas las transacciones de gas y petróleo están supervisadas por la NNPC (Nigerian National Petroleum Corporation), empresa controlada por el gobierno nigeriano. Cualquiera que quiera comerciar con petróleo en dicho país debe estar registrado en la NNPC.

En resumen este fraude funciona de la siguiente forma: El timador se pone en contacto con un bróker / intermediario ofreciéndole una gran cantidad de BLCO, entre uno y dos millones de barriles, a un precio muy atractivo.

Una vez el potencial comprador muestra su interés solicitará documentación que pruebe la existencia del producto (Proof of Product). Hay todo tipo de documentos que se pueden aportar, como certificados de calidad, certificados de origen, manifiestos de carga, o el ATS (Authority to Sell) otorgado por la NNPC.

Para cerrar el acuerdo, el comprador debe adelantar una importante suma de dinero, entre 50 y 100 mil dólares. Una vez pagada esta cantidad irá a recoger el petróleo y se encontrará con que lo han timado.



El punto más débil de este fraude está en la documentación que el timador debe presentar para convencer al comprador. Si bien todos estos documentos pueden falsificarse, se arriesgan a que el bróker trate de comprobar que efectivamente está todo en regla, pudiendo darse cuenta del engaño.

Para conseguir el golpe perfecto, los timadores deberían utilizar documentos reales, de tal forma que si el comprador verifica por su cuenta su veracidad se encontrará con que todo es real.

¿Pero cómo conseguir estos documentos? Realmente complicado. Para hacerlo habría que comprometer a empresas del sector que, por ejemplo, se encarguen del transporte del petróleo. Es una teoría, hasta ese momento no teníamos pruebas de que los responsables de "La Amenaza Fantasma" tuvieran este objetivo.

¿Se puede averiguar quién está detrás de este ataque?

En la mayoría de ataques averiguar quién está detrás es realmente complejo, en muchos casos es irrealizable.

No teníamos grandes esperanzas aquí, el hecho de no haber utilizado malware además nos quitaba la posibilidad de que hubiera firmado de alguna forma el ataque. Pero el cómo se había llevado a cabo el robo de información tenía un punto débil: la conexión por ftp para enviar las credenciales sustraídas.

La transmisión se realiza a través del comando ftp, y al ser llamado desde uno de los scripts, podemos ver la conexión que realiza, a dónde la realiza y qué credenciales utiliza para ello. El servidor ftp pertenece a un servicio gratuito en el que el atacante ha abierto una cuenta, así que pudimos acceder al mismo y ver la información que había utilizado en el registro de la cuenta. Es cierto que la información sería con toda seguridad falsa, pero nada perdíamos por comprobarlo.

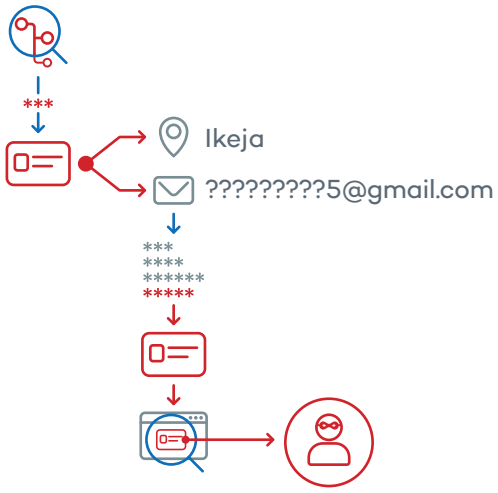
El nombre utilizado era falso, una búsqueda en Google devolvía cero resultados. Como país había puesto EEUU, algo que podía ser perfectamente inventado. Llegamos entonces a la ciudad. En este campo utilizó un nombre que no nos resultaba conocido: "Ikeja".

Resulta que Ikeja es un barrio de Lagos, capital de Nigeria, conocido también como "computer village" debido a un gran mercado de componentes informáticos que existe allí. Esta información podría ser también falsa, pero el hecho de que quien creó la cuenta conocía el nombre de "Ikeja" significaba que bien era nigeriano, o que conocía lo suficientemente bien el país para haber utilizado el nombre de un barrio desconocido para todos aquellos no familiarizados con Nigeria.

Finalmente llegamos a la dirección de correo. Es el único elemento de toda la información que sabemos con certeza que debe funcionar. En esa dirección recibirás el mensaje para activar tu cuenta, y la necesitarás si en algún momento necesitas la contraseña, por ejemplo. Se trataba de una cuenta de Gmail: *********5@gmail.com

La contraseña era desconocida, no había utilizado la misma que para el servicio ftp. Tomamos los 9 caracteres que estaban en la dirección de correo, y comenzamos a jugar con ellos para ver si podían formar un apodo, un nombre, apellido o similar. **Y dimos con ello**.

Buscamos en Google lo que parecía que podía ser un nombre y apellido y obtuvimos un resultado. Se trataba de una persona originaria de Nigeria. Tenía cuentas en redes sociales como Twitter, Facebook o LinkedIn, por lo que pudimos obtener algo más de información a través de ellas. Se trataba de alguien que vivía en... Ikeja. Y además es el supuesto dueño de una empresa que se encarga de transporte de mercancías. Demasiadas casualidades.



Sin embargo, aunque todo apunta a que se podría tratar de la persona detrás del ataque, no tenemos forma de probarlo. Sería necesario que la policía comenzara a investigar y pedir información de conexiones al ftp, etc. para tratar de obtener la dirección IP de quien se registró en el servicio y tratar de relacionarlo con el culpable.

Conclusión

Una vez recopilamos toda la información teníamos claro qué había que hacer: poner en conocimiento de la policía nuestro hallazgo para que pudieran investigar y a poder ser detener a los culpables de este ataque. Como una de las empresas afectadas era española, contactamos con la Guardia Civil. Con quienes hemos trabajado en numerosas ocasiones y que cuentan con un gran prestigio en la investigación de delitos digitales.

Lamentablemente se encontraron con un problema que no tiene fácil solución: para poder iniciar una investigación, necesitan que haya al menos una víctima que denuncie el delito. Algo que podría parecer sencillo no lo es tanto, y de hecho **ninguna de las víctimas ha querido presentar una denuncia**.

¿Por qué? Si nuestra teoría es correcta, la información robada a estas empresas no se ha utilizado para perjudicarlas, sino para timar a otras personas, los compradores de petróleo.

Es por eso que las empresas cuyas credenciales han sido comprometidas prefieren no correr el riesgo de denunciar el caso y que el nombre de su empresa salga a la luz. Prefieren cambiar las credenciales y seguir como si nada hubiera pasado. En algunos países existe legislación que obliga a las empresas a denunciar cuando han sufrido una intrusión en la que ha sido sustraída información. Sin embargo, esta obligación suele estar limitada a cuando a la empresa le ha sido sustraída información de terceros (clientes, socios, etc.). En el caso que nos ocupa, las credenciales robadas pertenecían a la propia empresa afectada, por lo que la legislación no fuerza a presentar una denuncia.

Comenzamos llamando a este caso "La Amenaza Fantasma", debido a las características del ataque y la ausencia de malware utilizado en el mismo. Siguiendo con el homenaje a La Guerra de Las Galaxias, es hora de ir a por "El Despertar de La Fuerza": todas las grandes compañías deben despertar y percatarse del hecho de que su seguridad nunca va a ser absoluta, y de que la seguridad basada en comportamiento es limitada. Es necesario ir un paso más allá, y realizar auditorías periódicas que permitan conocer el estado de la red y sus puntos más vulnerables. A pesar de que las soluciones tradicionales de seguridad son necesarias, no son suficientes. Nuestras defensas deben adaptarse al nivel de ataques que recibimos, por lo que hay que aplicar nuevas estrategias de protección que nos permitan tener un control absoluto de lo que sucede en nuestra red.

Las empresas como Black Gold prefieren no denunciar para que sus ataques permanezcan en el anonimato.