Ministerio del Interior

interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/13552853

La Guardia Civil desarticula una importante red dedicada a cometer estafas a través de Internet

Guardia Civil

Ribeira (A Coruña), Madrid, Parla y Móstoles (Madrid), Seseña (Toledo), Villafranca de los barros (Badajoz) y Aranda de Duero (Burgos), 10/07/2021

- Imágenes (2)
- Vídeos (0)
- Audios (0)

No existen vídeos relacionados con la noticia.

No existen audios relacionados con la noticia.

Se ha detenido a 16 personas en Ribeira (A Coruña), Madrid, Parla y Móstoles (Madrid), Seseña (Toledo), Villafranca de los barros (Badajoz) y Aranda de Duero (Burgos) por los presuntos delitos de estafa y pertenencia a organización criminal

A través de un software malicioso, instalado en el ordenador de la víctima por la técnica conocida como "email spoofing", habrían conseguido desviar a sus cuentas grandes cantidades de dinero

Los agentes han conseguido bloquear tentativas de transferencias por un importe de 3.500.000 euros, después de analizar más de 1.800 correos electrónicos

La Guardia Civil, en el marco de la operación AGUAS VIVAS, ha desarticulado una organización delictiva dedicada a cometer estafas a través de Internet. A través de un software malicioso, instalado en el ordenador de la víctima por la técnica conocida como "email spoofing", habrían conseguido desviar a sus cuentas grandes cantidades de dinero.

Se ha detenido a 16 personas en Ribeira (A Coruña), Madrid, Parla y Móstoles (Madrid), Seseña (Toledo), Villafranca de los barros (Badajoz) y Aranda de Duero (Burgos) por los presuntos delitos de estafa y pertenencia a organización criminal.

Se han esclarecido 20 delitos de estafa, por un importe total defraudado de 276.470 euros, de los cuales han podido ser recuperados 87.000 euros.

Asimismo, se han realizado 2 registros en Madrid, en los que han intervenido gran cantidad de documentación, dispositivos móviles y equipos informáticos.

La investigación se inició hace más de un año, tras varias denuncias presentadas por diferentes organismo oficiales, situados a lo largo de toda la geografía nacional, por la supuesta infección de sus equipos informáticos con algún tipo de software malicioso, con el que habrían conseguido desviar de sus cuentas, a través de la banca online, grandes cantidades de dinero.

Tras analizar los equipos informáticos afectados, los agentes observaron que la infección se llevaba a cabo a través de una técnica conocida como "email spoofing", consistente en el envío fraudulento de correos electrónicos en los que los atacantes ocultaban la verdadera dirección del remitente, sustituyéndola por otra, aparentemente, legítima, logrando así suplantar la identidad de organismos estatales como la Agencia Tributaria, Hacienda, Correos o la DGT.

Modus operandi

Los denunciantes recibían en sus cuentas de correo electrónico unos mensajes, supuestamente provenientes de organismos oficiales como la Agencia Tributaria, Hacienda, Correos, DGT, etc., en los que se les requería pagar deudas fiscales, abonar multas de tráfico, o la recogida de paquetes, para lo cual debían abrir un enlace inserto en el correo recibido para ver los detalles. Cuando accedían a ese enlace, en realidad estaban accediendo a una dirección o página web desde la que, en segundo plano, era descargado e instalado el programa malicioso.

Una vez instalado en el ordenador, sin que el usuario se diera cuenta, permanecía latente a la espera de ser activado en el momento en que el usuario accediera a cualquier página web de un banco, ejecutando una transacción bancaria. En ese momento el software malicioso realizaba una interceptación y modificación de los datos emitidos, consiguiendo que las cuentas beneficiarias del dinero fueran un total de 30 cuentas bancarias pertenecientes a la red. Tras ello, el dinero era diversificado mediante su envío a otras cuentas, o mediante extracción de efectivo en cajeros, transferencias por BIZUM, tarjetas REVOLUT, etc., con el fin de dificultar la posible investigación policial.

Una característica en la que coincidían todas la víctimas es que, una vez que realizaban cualquier operación bancaria a través de la web, sus ordenadores se reiniciaban varias veces hasta bloquearse el acceso, comprobando más tarde que se habían realizado transferencias de grandes cantidades de dinero a cuentas de desconocidos.

68 cuentas de correo electrónico infectadas por troyanos

Los investigadores, en colaboración con el Departamento de Informática de la Diputación Provincial de Cáceres, detectaron una actividad sospechosa en al menos 68 cuentas de correo electrónico pertenecientes a organismos oficiales, los cuales estaban infectados con los troyanos "Mekotio" y "Grandoreiro", y que permanecían a la espera de consumar las

transferencia fraudulentas. Los agentes han conseguido bloquear tentativas de transferencias por un importe de 3.500.000 euros, después de analizar más de 1.800 correos electrónicos.

La organización estaba perfectamente estructurada y jerarquizada, en 4 niveles. Por un lado se hallaban los que se dedicaban a recibir las cantidades de las transferencias fraudulentas (Nivel 1), que posteriormente transferían a otros miembros de la organización (Nivel 2). Por otro lado, se encontraban los que transferían el dinero a otras cuentas ubicadas en el extranjero (Nivel 3) y, finalmente, los que se dedicaban a enmascarar la operativa online de las cuentas (Nivel 4).

Phishing, Vishing y Smishing

Se tratan de tres ataques basados en ingeniería social muy similares en su ejecución. De forma general, el ciberdelincuente enviará un mensaje suplantando a una entidad legítima, como puede ser un banco, una red social, un servicio técnico o una entidad pública, con la que nos sintamos confiados, para lograr su objetivo. Estos mensajes suelen ser de carácter urgente o atractivo, para evitar que aplique el sentido común y se lo piensen dos veces.

- **Phishing**: Suele emplearse el correo electrónico, redes sociales o aplicaciones de mensajería instantánea.
- **Vishing**: Se lleva a cabo mediante llamadas de teléfono.
- **Smishing**: El canal utilizado son los SMS.

En ocasiones, traen consigo un enlace a una web fraudulenta, que ha podido ser suplantada, fingiendo ser un enlace legítimo, o bien se trata de un archivo adjunto malicioso para infectarnos con malware.

Su objetivo es obtener datos personales y/o bancarios de los usuarios, haciéndonos creer que los estamos compartiendo con alguien de confianza. También pueden utilizar esta técnica para que descarguemos malware con el que infectar y/o tomar el control del dispositivo.

Recomendaciones

El principal consejo es ser precavido y leer el mensaje detenidamente, especialmente si se trata de entidades con peticiones urgentes, promociones o chollos demasiado atractivos.

Además, otras pautas que podemos seguir para evitar ser víctima de este tipo de engaños, pueden ser:

- Detectar errores gramaticales en el mensaje. Y, si se trata de un asunto urgente o acerca de una promoción muy atractiva, es muy probable que se trate de un fraude.
- Revisar que el enlace coincide con la dirección a la que apunta. Y, en cualquier caso, debemos ingresar la url nosotros directamente en el navegador, sin copiar y pegar.

- Comprobar el remitente del mensaje, o asegurarnos de que se trata de un teléfono legítimo.
- No descargar ningún archivo adjunto y analizarlo previamente con el antivirus.
- En caso de vishing, no debemos descargar ningún archivo que nos haya solicitado el atacante, ni ceder el control de nuestro equipo por medio de algún software de control remoto.
- No contestar nunca al mensaje y eliminarlo.

La operación, dirigida por el Juzgado de Primera Instancia e Instrucción nº. 1 de Cáceres, ha sido llevada a cabo por agentes pertenecientes al Equipo de Delitos Tecnológicos (EDITE) de la Unidad Orgánica de Policía Judicial (UOPJ) de la Comandancia de Cáceres.

Para más información pueden contactar con la Oficina Periférica de Comunicación de la Guardia Civil de Cáceres, en el teléfono **680.410.422**.

Existen imágenes de vídeo, a disposición de los medios que las deseen, en el siguiente enlace:

www.guardiacivil.es/es/prensa/videos_descarga_medios/2021/index.html