GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

GUARDIA CIVIL
DIRECCIÓN ADJUNTA OPERATIVA
MANDO DE OPERACIONES
JEFATURA DE POLICÍA JUDICIAL
UNIDAD TÉCNICA DE POLICÍA JUDICIAL

DOCUMENTO
DE ANÁLISIS
DE RIESGOS
Y DIFUSIÓN
OPERATIVA

DARDO

2/2016

ESTAFAS AL SECTOR EMPRESARIAL MEDIANTE TÉCNICAS DE INGENIERIA SOCIAL "FRAUDE AL CEO"

Madrid, 03 de marzo de 2016

1. ANTECEDENTES

Del análisis de la información disponible en la Jefatura de Policía Judicial-Unidad Técnica de Policía Judicial (UTPJ), procedente de diferentes investigaciones efectuadas por las Unidades de la Guardia Civil, foros internacionales como Europol e Interpol, así como de relaciones bilaterales mantenidas con otros operadores de seguridad y agencias policiales, se ha podido constatar la existencia de nuevas tendencias y "modus operandi" en el campo de estafas a través de las nuevas tecnologías.

En este caso se va a analizar la estafa conocida como **"Fraude al CEO (*CEO Fraud*),** en el que las organizaciones criminales, empleando técnicas de ingeniería social y "hacking" *(explotación de las vulnerabilidades de los sistema de información, para acceder a ellos de manera ilícita con diversos fines, principalmente el robo de datos)* y comprometiendo las comunicaciones de las empresas, engañan a los responsables de las mismas para conseguir un beneficio económico de naturaleza ilícita.

2. ANÁLISIS DE LA PROBLEMÁTICA

2.1.- Introducción.

El uso cada vez más extendido de internet y la mayor dependencia que tienen de la red los diferentes actores sociales, lleva a ampliar el espectro de objetivos susceptibles de ser víctimas de estafas *online* por parte de los delincuentes y de las organizaciones y grupos criminales.

Ello se ve reforzado por la continua evolución en las técnicas y procedimientos de los delincuentes, así como en la permanente búsqueda de nuevas tipologías de víctimas sobre los que orientar sus actividades.

En este proceso de adaptación se ha evidenciado la especialización de las organizaciones criminales en el uso del conocido "*crime-as-a-service*"[1], donde se observa una carga de especialización en técnicas de *hacking* en beneficio del empleo de *ingeniería social*.

[1] Delincuentes especializados en el desarrollo de herramientas (en este caso informáticas) concretas, que son subcontratados o cuyas herramientas son adquiridas para la explotación de alguna vulnerabilidad específica en beneficio de la organización criminal. Quien realiza el daño o el hecho criminal no es el que ha creado la solución concreta para ello, sino quien la ha comprado.

2.2.- Ingeniería social

Para entender el proceso de engaño mediante el Fraude al CEO, es necesaria una aproximación previa al concepto de "*ingeniería social*".

Se entiende como tal la aplicación intencionada de técnicas de engaño orientadas a manipular a una persona para que, bien aporte información sensible, bien se le induzca a llevar a cabo a cabo acciones inconscientes cuyo resultado es la obtención de esa misma información por parte del atacante o que la víctima efectúe alguna acción que finalmente le resulta perjudicial.

Se puede dividir en dos categorías según el grado de interacción con el objetivo:

- La primera de ellas conocida como "*hunting*", se lleva a cabo cuando la interacción es mínima, es decir, se intenta acceder a la información con el mínimo contacto víctima-atacante (p.e correos electrónicos puntuales simulando proceder de una entidad bancaria de la que la víctima es usuario).

- La segunda de ella, denominada "*farming*", requiere una relación continua entre el delincuente y la víctima para basar la cesión de esos datos en una relación de confianza (P.e. mediante la creación de perfiles falsos en RRSS por parte de los estafadores y la posterior comunicación con los objetivos).

Los principales vectores de ataque, es decir los medios a través de los cuales se infiere a la víctima a realizar una acción perjudicial para él, son por lo general sitios web comprometidos, correos electrónicos, vía teléfono (normalmente llamadas VoIP[2] o servicios de mensajería para móvil) y servicio postal tradicional (casi en desuso).

En referencia a los métodos empleados (unos con mayor carga técnica y otras donde la ingeniería social es más elaborada) a través de estos vectores de ataque destacan:

- ***Phising***.- El más extendido y usado por los estafadores. Es la simulación de una página web determinada para inducir al objetivo a cargar determinados datos personales. Normalmente son diseminados mediante correos electrónicos tipo *spam*.
- **Spearphising.-** Modalidad de *phising* donde el engaño está mucho más elaborado. En este caso la víctima recibe un correo electrónico de

[2] VoIP.- Conjunto de recursos que permiten la trasmisión de señal de voz por la red mediante protocolo IP.

una contacto de confianza, invitándole a realizar alguna acción que le ocasiona perjuicio directo o indirecto.

- ***Whaling*.-** *Spearphising* mucho más trabajado dirigido a ejecutivos de alto nivel o a personal con cargos relevantes que usualmente gestionan información corporativa sensible.
- ***Pretexting.-*** En este caso prevalece la carga de la ingeniería social sobre la técnica. El estafador necesita una información concreta por lo que inventa escenarios que induzcan a la víctima a aportar esos datos. Se basa la actuación en una mentira elaborada donde normalmente el atacante llega a crearse una identidad falsa para manipular a su objetivo.
- ***Baiting.-*** Modalidad de ingeniería social que basa su engaño en tentar al objetivo con algún objeto o servicio de su interés. El clásico ejemplo son los supuestos servicios de descarga de películas o música donde piden previamente determinados datos personales.
- ***Quid pro quo***.- Técnica de ingeniería social que promete un beneficio a cambio de algo. Ejemplo claro es el estafador que se hace pasar por técnico del área de las TIC que ofrece sus servicios gratuitamente a cambio de adquirir un antivirus determinado, estando este último infectado por algún troyano.
- ***Tailgating***.- Variante de ingeniería social cimentada en el abuso de confianza. De forma muy general, se basaría en ganar la confianza de la víctima para lograr la cesión su dispositivo (teléfono, ordenador) con alguna excusa, y una vez en su poder, instalar algún tipo de malware para el robo de datos.

Para lograr el acceso a la información de las víctimas, los delincuentes intentan adecuar el ataque al objetivo mediante el siguiente proceso:

1. **Fase de investigación**. Se intentan obtener todos los datos relativos a la víctima que puedan servir para identificarla y centrarla. Normalmente se acude a la información contenida en fuentes abiertas, como webs corporativas, perfiles en RRSS o documentos públicos, pero dependiendo de las capacidades, también se puede realizar incluso un control físico de la víctima. En el caso de dirigirse el ataque a una empresa, se identifica al empleado que tenga acceso a la información sensible.

2. **Fase de contacto**. Es el momento de acercarse e implicar al objetivo, presentándole el engaño como punto de partida para ganar su confianza.

3. **Fase de obtención**. Se procede a explotar la relación extrayendo la información buscada de la víctima mediante el abuso de esa vinculación de confianza, bien de forma directa, bien induciendo al objetivo una actuación específica (p.e. acceder a un sitio web comprometido mediante un “link”).

4. **Fase de salida.** En este periodo se culmina la interacción con el objetivo, una vez obtenida la información necesaria. Para terminar el engaño con éxito, el estafador procura que la víctima no sea consciente de la situación.

2.2.- Estafas sector empresarial. “CEO Fraud”

Las organizaciones criminales dedicadas a enriquecerse mediante la comisión de estafas en la red, están centrado su actuación en el sector privado.

Se han dado cuenta que haciendo un trabajo previo de inteligencia, en lugar de enviar los tradicionales correos electrónicos "*spam"* indiscriminados a todo tipo de usuarios, pueden obtener beneficios mucho mayores efectuando ataques más dirigidos.

Por ello, los ciberdelincuentes están focalizando su actividad en objetivos "de alto valor", como son los directivos de la empresas, que tienen capacidad de gestionar operaciones económicas o con poder de decisión sobre ellas.

La actividad criminal comienza con la identificación de la empresa y persona víctima, alternando análisis de fuentes abiertas (la disponibilidad de esta información aumenta peligrosamente la posibilidad de sufrir este tipo de ataques, aun sin estar perpetrados por delincuentes excesivamente especializados) con observación física, para fijar al directivo que pueda tener un control o responsabilidad sobre asuntos financieros y capacidad de decisión y/o ejecución sobre ellos.

El paso siguiente va orientado a comprometer el correo electrónico corporativo a través de técnicas hacking (desarrollo de malware *ad hoc*, empleo de vulnerabilidades concretas de navegadores o ataques “*watering hole*”[3]), explotándolos posteriormente mediante el uso de ingeniería social contra los directivos (consejeros delegados, personal con poder de decisión en el ámbito económico, directores ejecutivos...).

De lo que se trata en suma es de, mediante engaño, obtener información sobre el directivo para después hacerse pasar por él y efectuar una operación económica en su nombre o bien obligarle a que sea éste quien la haga de manera inconsciente.

[3] Colocación de exploits en páginas web frecuentadas por la víctima, para en el caso de acceder a ellas, descargarse un código dañino en el dispositivo.

Los estafadores consiguen por tanto comprometer las cuentas de correo electrónico de las empresas y sus directivos. Una vez que se tiene acceso a la información corporativa y a la forma de trabajar, los delincuentes lo explotan.

Como ejemplo de estas técnicas de ingeniería social, se ha detectado como intentan convencer al CEO de una compañía para enviar un email con datos de sus empresas suministradoras, simulando ser un miembro del *staff* de una gran auditora, con la que evidentemente han tenido relaciones profesionales. Una vez obtenidos estos datos, los trabajan elaborando patrones de comunicación imitados (horas de orden de emisión de pagos, fórmula de pago, redacción de correos…) para suplantar al proveedor y comunicarse con el directivo sin que dé cuenta de la suplantación.

El fin último es poder simular una comunicación (por ejemplo mediante técnicas de *spoofing*[4]) para conseguir que el directivo ordene transferencias de fondos no autorizadas. Estos fondos son enviados a terceros estados como China y Hong Kong.

Sobre la base de lo anterior, destacan ente otros los siguientes *modus operandi*:

- ***Tipo 1. Suplantación empresa proveedora***

  En este caso la empresa víctima realiza una solicitud de productos a un proveedor de confianza . Como en una relación normal entre empresas, el proveedor estudia la solicitud y responde a la empresa solicitante con la aceptación del pedido.

  Posteriormente los estafadores, que se encuentran monitorizando la transacción, contactan con la empresa víctima solicitante del pedido a través del correo electrónico para, haciéndose pasar por el proveedor, por ejemplo, cambiar la cuenta de pago de la factura (normalmente a un banco de un tercer estado como China u Hong Kong). En la mayoría de los casos, la organización criminal se comunica desde un correo electrónico con un dominio muy similar, donde muchas veces no se aprecia la diferencia (p.e. "customer@**company**.com" en lugar de "customer@**co**n**pany**.com").

  La empresa víctima, creyendo que el remitente es la compañía real y pensando que está efectuando la transferencia a su proveedor de confianza, procede con el envío del pago a la nueva cuenta bancaria que le han comunicado en el correo. Cuando la empresa comunica a su proveedor que ya

[4] Ataque de suplantación basado en el acceso ilegitimo a recursos de un determinado sistema que ha establecido algún tipo de confianza basado en el nombre o la dirección IP de un *host* determinado.

ha efectuado el pago en la nueva cuenta, estos le responden que no han recibido el pago y que no han cambiado dicha cuenta bancaria.

- ***Tipo 2. La empresa recibe una solicitud de transferencia bancaria***

En este caso, la organización criminal realiza un análisis sobre los cargos ejecutivos de una compañía, con la intención de localizar un objetivo que tenga capacidad para manejar información confidencial y emitir determinadas órdenes de trabajo. Una vez identificado, le hacen un estudio (más o menos detallado dependiendo de la entidad del ataque) de sus costumbres. Centran su actividad en un control físico, estudiando las redes Wifi a las que se conecta (especial atención a las públicas) y dispositivos que usa (principalmente BYOD[5]), centrando los sitios web que frecuenta y grado de securización que implementa en sus comunicaciones.

Posteriormente, mediantes técnicas de *hacking* y de ingeniería social acceden a la cuenta oficial para identificar contactos y patrones de comportamiento. Una vez observado el flujo de las comunicaciones falsifican la cuenta de correo electrónico del ejecutivo de la empresa, enviando en su nombre a un empleado capacitado para realizar las trasferencias bancarias una solicitud de transferencia bancaria urgente a una cuenta controlada por los delincuentes. Empleando de nuevo el engaño, presionan con diferentes pretextos al trabajador en nombre del directivo (normalmente se intenta aprovechar una ausencia o circunstancia que tenga problemas de comunicación) argumentando normalmente razones de urgencia

- ***Tipo 3. Correo electrónico de un empleado de la empresa***

Los estafadores acceden ilícitamente el correo electrónico de un empleado de la empresa víctima con capacidad de solicitar los pagos de las facturas a sus clientes.

El grupo criminal envía diferentes requerimientos de pago de las facturas pendientes a empresas clientes usurpando el correo electrónico corporativo del empleado, identificados a partir de la lista de contactos de la cuenta de dicho trabajador y del análisis de su contenido. En el contenido del mensaje aportan un cambio de cuenta bancaria o de modo de pago en beneficio de los delincuentes.

[5] Tecnología *Bring Your Own Device* (BYOD), política corporativa consistente en integrar en dispositivos particulares aplicaciones y soportes profesionales para tener acceso a recursos de la empresa.

De esta forma, existe una doble victimización, por un lado la empresa que es suplantada, y por otro lado la de la compañía cliente que realiza el pago a un tercer individuo ajeno a toda relación comercial.

2.4.- Perfil de las víctimas de estas estafas.

Para la búsqueda de un mayor lucro, las organizaciones criminales focalizan cada vez más su actividad en el sector empresarial, tanto en grandes corporaciones como en las Pequeñas y Medianas Empresas (PYMEs).

En este último caso, el hecho de tener capacidad de mover flujos de dinero mayores que los usuarios particulares, y por otro, un previsible menor gasto en inversión para medidas de protección y securización de la información corporativa que las grandes empresas, los transforman en objetivos provechosos susceptibles de ser víctimas de este tipo de estafas.

El perfil de las empresas víctima es muy general, centrándose la actividad criminal principalmente en compañías de índole logístico y de comercio, muy especialmente vinculadas a negocios internacionales.

3. RECOMENDACIONES OPERATIVAS

El abandono paulatino de los tradicionales sistemas de comunicación en beneficio de las nuevas tecnologías buscando una mayor agilidad y fluidez, puede llevar a dejar en segundo plano la protección del medio y la autentificación de los interlocutores, favoreciendo en gran medida la actividad de estos delincuentes.

A la vista de lo anterior, pueden adoptarse una serie de medidas que sirvan para evitar o, en su defecto, minimizar el impacto de este tipo de hechos, para facilitar las investigaciones posteriores, así como, para el estudio de su evolución:

- Implementar en la empresa, en lo posible, medidas de seguridad informática.

- Formar a los directivos y responsables, sobre la necesidad de asumir un cultura de seguridad en las comunicaciones, prestando especial atención a la cesión de datos sensibles a través de los sistemas.

- Prestar especial atención a la hora de efectuar operaciones de naturaleza económica (pagos). En particular y por ejemplo:

    - Si se trabaja con proveedores extranjeros, contactar telefónicamente con el encargado de la empresa para corroborar los posibles cambios en la forma de abono, ante la posibilidad de encontrarse comprometido el email oficial.
    - Si un empleado recibe una solicitud de transferencia por parte de uno de sus superiores, a través del email, comprobar que dicha información es veraz por una tercera vía.
    - Si la empresa recibe un correo de su proveedor cambiando el número de cuenta donde, normalmente, recibe el pago de las facturas, es conveniente contactar con dicho proveedor para ratificar el cambio de cuenta.

- Informar al sector empresarial acerca de la necesidad de comunicar a la Guardia Civil cualquier incidencia sospechosa, y de conservar la información vinculada a las transacciones/comunicaciones durante un tiempo prudencial, por si fuera de utilidad en investigaciones.

- Solicitar de las empresas afectadas los preceptivos informes sobre el impacto económico derivado para adjuntarlo a la denuncia.

GUARDIA CIVIL

DARDO

DOCUMENTO DE ANÁLISIS DE RIESGOS Y DIFUSIÓN OPERATIVA