ROOT-SECURE
SECURITY MAKERS

Ingeniería Social
¿ Estamos Preparados ?

Índice

Que es la Seguridad de la Información.

Ingeniería Social.

Objetivo

Técnicas

Definición de ataques

Tendencias

Recomendaciones

Que es Seguridad de la Información

La seguridad de la información tiene como objetivo principal proteger los datos de las empresas , debe responder a tres cualidades principales Critica , Valiosa y Sensible.

La seguridad de la información, como concepto, se basa en **cuatro pilares**: la disponibilidad, la integridad, la confidencialidad y la autenticación.

- **Confidencialidad.**
- **Disponibilidad.**
- **Integridad.**
- **Autenticación.**

Ingeniería Social

La Ingeniería social es una técnica que utilizan los ciberdelicuentes para obtener información confidencial de sus victimas a través de metodologías engañosas .

Los principales conceptos a tener en cuenta son :

El usuario es el eslabón para débil de la cadena.

La habilidad del atacante para conseguir que su victima le proporcione los datos confidenciales.

La Creatividad del Atacante.

.

Objetivo

El objetivo del atacante es obtener datos sensibles . Los ciberdelincuentes intentan engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, se hacen pasar por familiares, personas de soporte técnico, compañeros de trabajo o personas de confianza. El objetivo de este engaño es apropiarse de datos personales, contraseñas o suplantar la identidad de la persona engañada.

En esta etapa el atacante entra en conocimiento de la organización, o persona identificando el público objetivo y segmentándolo para optimizar el uso de los recursos:

- **Distribución geográfica**
- **Intereses específicos**
- **Nivel de responsabilidad**
- **Rangos etáreos**

Ingeniería Social - Técnicas

- **La ingeniería Social está definida como un ataque basado en engañar a un usuario o administrador de un sitio para poder ver la información que ellos quieren.**
- **Se hace para obtener acceso a sistemas o información útil.**
- **Los objetivos de la ingeniería social son fraude, intrusión de una red.**

- ❑ **Phishing.**
- ❑ **Vishing.**
- ❑ **Smishing.**
- ❑ **Tailgaiting o Piggybacking.**
- ❑ **Baiting.**
- ❑ **Shoulder Surfing.**
- ❑ **Escritorios Limpios.**
- ❑ **Fuentes Abiertas.**

Definición de Ataques

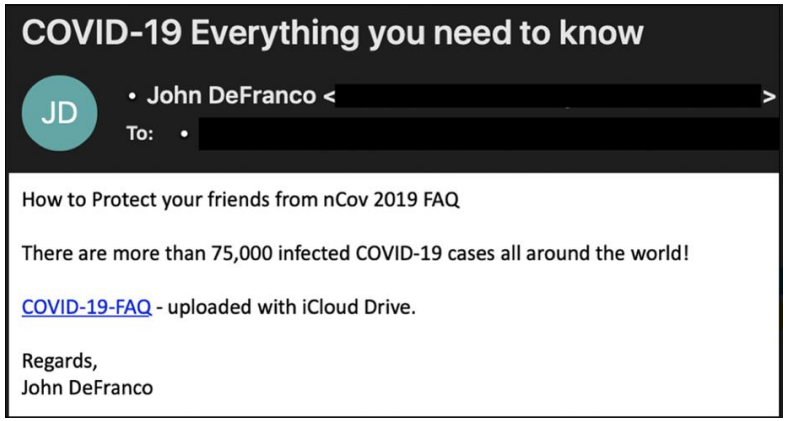
- **Fuentes Abiertas –** Este análisis pretende averiguar a través de las lecciones históricas cuáles son los pilares y características que moldean el OSINT. De este modo se entenderá mejor esta forma de inteligencia, y en particular sus grandes debilidades y posibilidades de explotación ante actores dispuestos a aprovecharlo para provocar el engaño.

.

Definición de Ataques

- **Phishing** – Envío de Correo .(Simulación de sitio Web) El atacante intenta engañar a su victima para que haga click en un enlace, descargue un archivo adjunto o envíe información solicitada con datos confidenciales o para que realice un pago.

.



Definición de Ataques

- **Vishing** – Es una estafa que se realiza a través de una llamada telefónica. En estas llamadas el atacante buscan engañar a los usuarios, haciéndoles creer diversas historias y situaciones que relatan a través del teléfono.

Origen del llamado	Info a obtener	Detalle
Llamado de Soporte	IP del equipo	Enviamos parches en la PC y necesitamos la IP del equipo para validar que se hayan instalado correctamente. Que nos pasen la IP del equipo

Origen del llamado	Info a obtener	Detalle
Llamado desde Sistemas	usuario y contraseña del usuario	Habla XXXXX de Sistemas, estamos haciendo una validación de usuarios y chequeando los usuarios activos. Necesito que me pases usuario y contraseña de Windows con la que estás trabajando en la PC.

Origen del llamado	Info a obtener	Detalle
Llamado desde Cadena de VEntas	Obtener usuario , DNI y datos sensibles	Habla XXXX de Telemarketing , están intentando realizar una compra por un monto elevado y queríamos confirmar la operación .

.

Definición de Ataques

- **Smishing** – Esta técnica se utiliza a través del envío de mensajes de teléfono móvil (SMS) para lograr que las víctimas tomen acciones inmediatas.

  El smishing es una amenaza emergente y en crecimiento en el mundo de la seguridad en línea. Es una estafa en la cual, por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número o que se entre a un sitio web.

.

Definición de Ataques

- **Tailgaiting o Piggybacking** – Esta técnica consiste en seguir a una persona a través de puertas que tienen cerraduras de acceso , intentar evadir los controles de seguridad a través de diferentes accesos o hasta ponerse un disfraz para engañar a las personas para que abran esa puerta

.

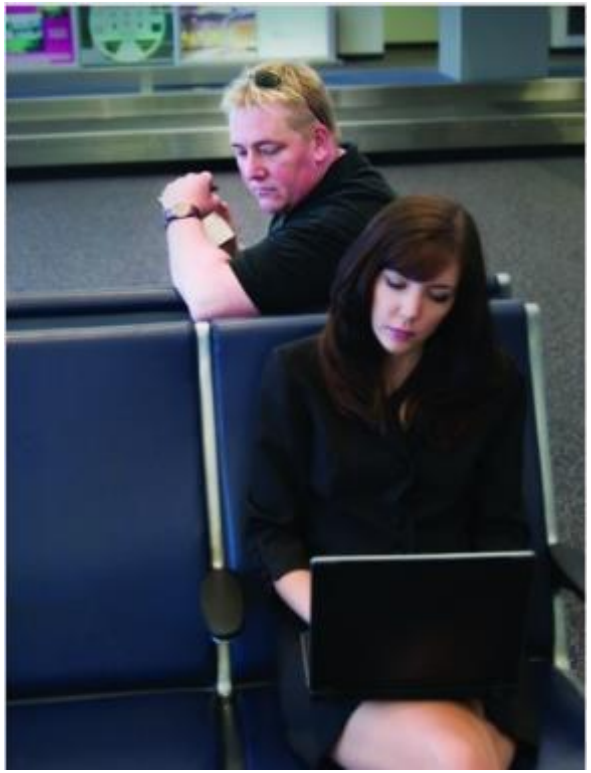
Definición de Ataques

- **Baiting –** Esta técnica se utilizan memorias flash (usb) infectadas con malware que son colocadas en diferentes sectores con el fin que este hardware se inserte en ordenadores conectados a redes como medio para diseminar el código malintencionado.

.

Definición de Ataques

- **Shoulder Surfing** – Esta técnica consistes en “ espiar” a la victima , esto se puedo lograrse al estar sentado cerca de la victima , escuchando conversaciones con el fin de detectar algún dato interesante , como se una clave , u observar la pantalla del dispositivo móvil o notebook mientras la victima esta ingresando datos.



.

Definición de Ataques

- **Escritorios Limpios –** En esta técnica el atacante una vez que accedió al escritorio de la victima procede a revisar el mismo en búsqueda de datos sensibles.

Definición de Ataques - Menores

- **Grooming–** Es un proceso en el que se produce un vínculo de confianza entre la víctima y el acosador. Este intenta aislar poco a poco al menor, y lo consigue desprendiéndolo de su red de apoyo (familiares, profesores, amigos, etc.) y generando un ambiente de secretismo e intimidad.
- En el caso del ***online grooming*** **el abusador** envía, a través de un medio tecnológico, material sexual al niño o niña. Además, **se suele hacer pasar por menor** y adapta el lenguaje a la edad de la víctima. Es una violencia igual de real que la física, pero de la que no se puede huir.

.

Definición de Ataques - Menores

Principales programas que utilizan los menores donde se llevan a cabo los ataques

- **Roblox.**
- **Minecraft.**
- **TikTok.**
- **Kwai.**
- **Fornite.**
- **Snapchat.**

Tendencias

- A la fecha los principales ataques de ingeniería social que se están llevando a cabo son

- ❑ Fraude Bancario (Telefónico)
- ❑ Robo de Aplicaciones de Mensajería Instantánea (whatsapp - Vacunas).
- ❑ Secuestros de Claves de Aplicaciones donde se maneja dinero.

.

Tendencias

- En el futuro próximo, uno de los objetivos de los atacantes será corromper los sistemas existentes en la nube para ganar acceso a ellos mediante campañas de phishing. Uno de los ejemplos más claros hoy en día es el uso de aplicaciones para acceder a Office 365 y G Suite por medio de alojamiento de software malintencionado que se encuentra embebido en correos electrónicos maliciosos y en enlaces públicos docs.google.com/, pues es poco probable que una organización bloquee un domino de Google.

.

Recomendaciones

- Identificar y evitar abrir archivos recibidos por correo electrónico de remitentes desconocidos, sobre todo si anexan instrucciones que normalmente no se realizan.
- Comparar los dominios entre el original y el posible sitio malicioso; identificar errores de ortografía en los correos electrónicos o sitios Web, así como los remitentes de correo electrónico desconocidos.
- No usar la misma contraseña en más de una cuenta, servicio o página.
- Realizar compras en sitios confiables y auténticos. Nunca hacer clic en enlaces embebidos en un correo electrónico o mensaje de redes sociales, hay que buscar el enlace del vendedor o del promocional por fuera, de manera directa.
- Desconfiar de las ofertas «imperdibles». Aquellas que ofrecen productos milagrosos o con descuentos muy atractivos.
- Las organizaciones deben evitar los ataques de día cero apostando por una infraestructura de protección de extremo a extremo que permita implementar políticas en el servidor de correo para evitar dominios fraudulentos, o en su caso filtrado web, y proporcionar alertas sobre la reutilización de contraseñas en tiempo real.
- Pruebas , Capacitación , y Re testeo a los usuarios de la empresa.
- Realizar una revisión profunda de los redes sociales de los menores.

PREGUNTAS ?

ROOT-SECURE

SECURITY MAKERS