Managed secure IT | no matter what

RIESGOS DE SEGURIDAD ROBO DE IDENTIDAD

www.mexis.net

Autor: Mariana Tapia y Luis Sánchez

1. RESUMEN EJECUTIVO

Hoy en día el acceso a internet se ha vuelto la principal fuente de información alrededor del mundo acompañado del e-commerce en lo relativo a las ventas por internet. En la medida que ha crecido estas dos grandes vertientes de la tecnología, lo mismo ha sucedido para el robo de identidad.

El robo de identidad es definido como cualquier clase de delito derivado de la pérdida o robo de datos personales, un dato personal se entiende como todo tipo de información que hace a una persona identificable o identificada y que te distingue de los demás, estos datos personales son clasificados por:

- Datos personales identidad
- Datos personales patrimoniales
- Datos personales de trabajo
- Datos personales de educación
- Datos personales de ideología
- Datos personales de salud
- Datos personales de características físicas
- Datos personales de intimidad

Uno de los robos de identidad más utilizados es el fraude por robo de contraseñas, nombres de usuarios, información bancaria o números de tarjeta de crédito, los cuales en casi todos los casos son clasificados como datos personales patrimoniales y que su vez son identificados como datos de credenciales bancarias ya que estos son el principal objetivo de un ataque cibernético.

Cifras indican que durante el primer trimestre del 2018 la CONDUSEF recibió más de un millón de reclamaciones en lo relativo al comercio electrónico, de la misma forma el Banco de México indicó que nuestro país ocupa el 8° lugar a nivel mundial de robo de identidad.

Especialistas mencionan que solo el 5 % y 7 % de los comercios e instituciones han implementado medidas de autenticación como el uso de mecanismos de Biométricos sin embargo la CONDUSEF comenta que no existen lineamientos que obliguen a los comercios a proteger los datos personales de los usuarios con mejores o mayores medidas de autenticación.

2. PRINCIPALES TÉCNICAS PARA LLEVAR ACABO EL ROBO DE CREDENCIALES BANCARIAS

Las estafas más comunes son realizadas por medio de las siguientes técnicas utilizadas por cibercriminales:

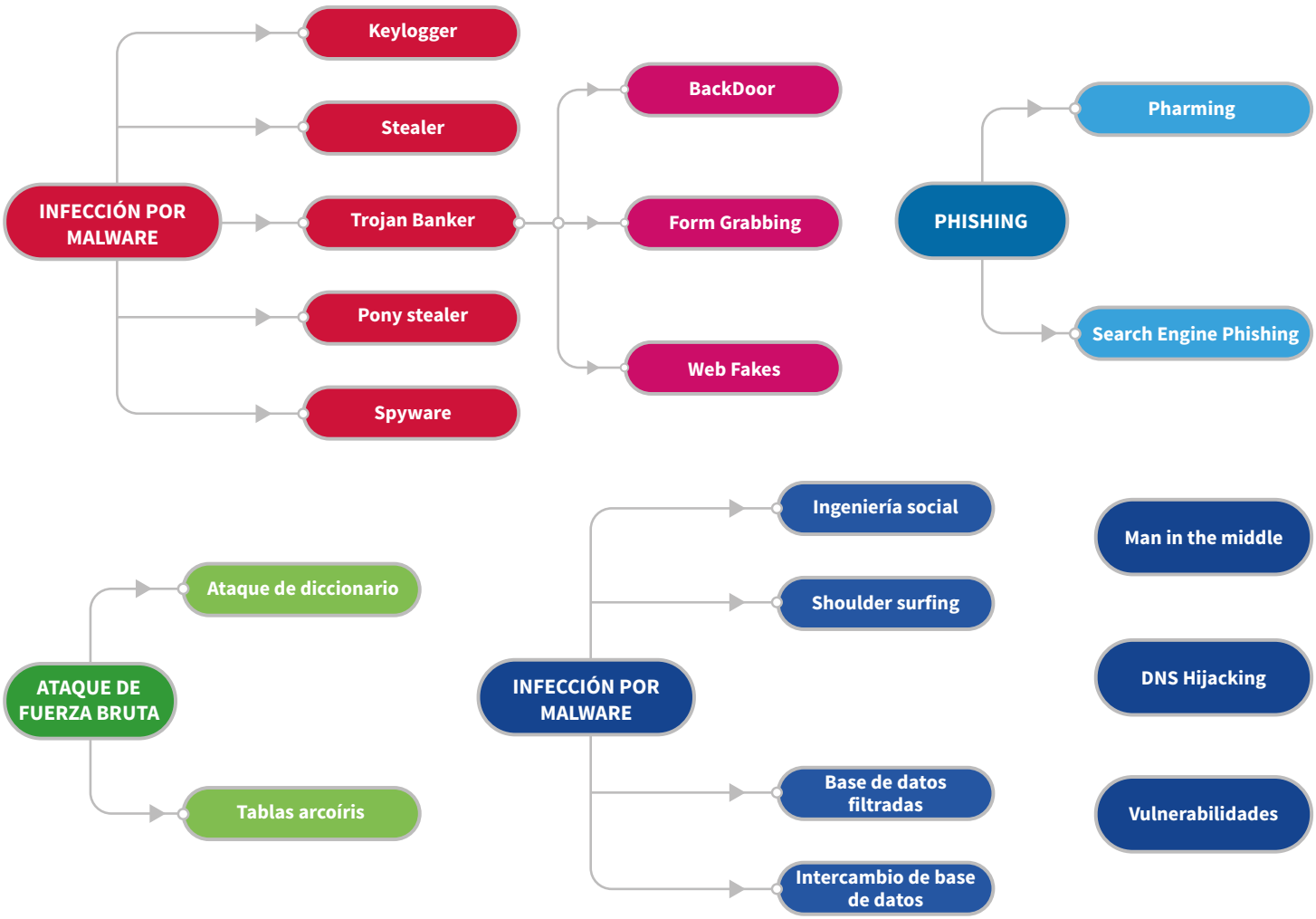


Fig. 1 Cuadro de técnicas utilizadas para el robo de credenciales bancarias

Los cibercriminales que llevan a cabo el robo de identidad generalmente no son los mismos que los usan, hay mercados vibrantes donde existen compradores y vendedores que acuerdan términos y condiciones de las ventas. El robo más persistente en la actualidad es el relacionado a los datos de credenciales bancarias (password, usuario, número de tarjeta de crédito o débito).

3. INFECCIÓN POR MALWARE

KEYLOGGER

Keylogger es un software o hardware que una vez instalado tiene la capacidad de registrar y memorizar toda la información que se ponga en el teclado, la forma en que se infecta el equipo es por medio de un programa que solicita ser instalado en la mayoría de los casos en anexado a un email o se puede guardar en una memoria USB para que posterior a su uso sea ejecutado de forma automática.

Su función principal es que cada vez que el usuario va tecleando información el software hace un registro de cada movimiento y genera una captura en su propio espacio de memoria o en su caso en el disco duro del equipo. El riego principal radica en que, al momento de teclear contraseñas, cuentas bancarias o algún NIP, el software realiza el almacenamiento y roba la información.

Hoy en día se puede acceder al software desde páginas Web comunes como softtonic.com, la principal protección contra este programa es la instalación de un buen antivirus que detecte este tipo de malware, de igual forma es muy recomendable que se utilicen barreras como es el firewall.

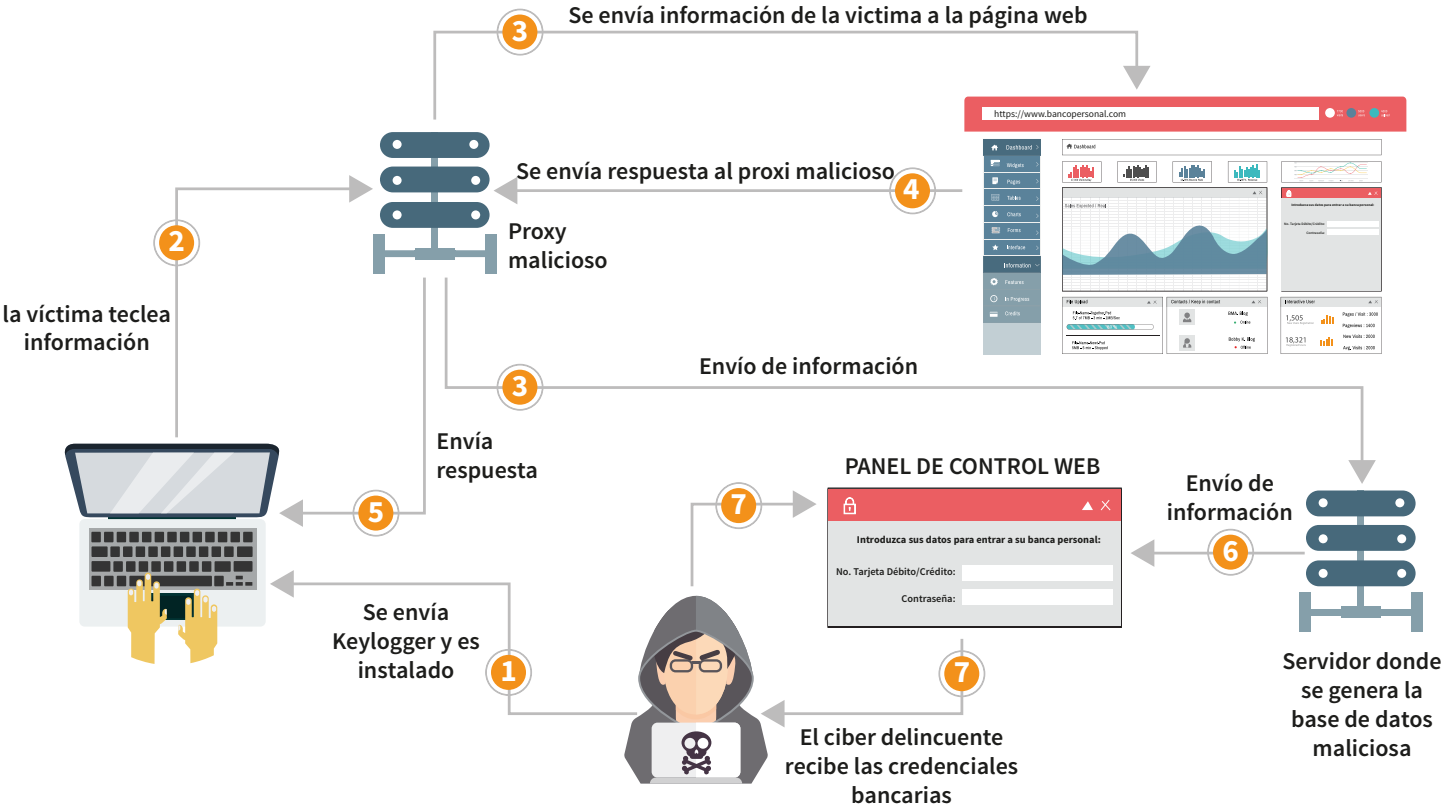


Fig. 2 Forma de operar de Keylogger

STEALER

Vega Stealer es un malware usado para el robo de credenciales bancarias, es una variante del virus August Stealer que fue detectada a través de una campaña de correo electrónico (Phishing) que por medio de un ejecutable se instala en carpetas del equipo. Su principal fuente de recolección de información es por medio de los navegadores.

En Chrome la actividad principal es la de extraer contraseñas, tarjetas de crédito guardadas (nombre, fecha de vencimiento y numero de tarjeta), cookies y perfiles de los usuarios.
En Firefox, recolecta los archivos de las carpetas donde se almacenan contraseñas y claves.

TROJAN BANKER

Trojan Banker es un troyano que está asociada con el Banload y Downloader. Banload troyano. Este troyano ataca a las PC´s de las víctimas a través de sitios Web que emplean driev-by, fue diseñado para monitorear las actividades de Pc´s de las víctimas, esto con el fin de robar los nombres de usuarios, contraseñas e información financiera/bancaria y sensible. Tiene la capacidad de abrir agujeros de seguridad en los sistemas para dejar libre el camino a otros tipos de malware para ganar una fácil entrada en el sistema. También se le puede encontrar como:

- **BACKDOOR**
- **FORMGRABBING**
- **WEBFAKES**

BACKDOOR

Es un programa malicioso de ordenador utilizado para proporcionar un acceso remoto de las PC´s al atacante, una vez dentro realiza una explotación de vulnerabilidades del sistema. Funciona en el segundo plano del sistema y se esconde del usuario, lo que hace que sea difícil de ser encontrado, esta considerado como uno de los virus más peligrosos, ya que su uso principal es del espiar en archivos o carpetas, toma el control de la administración de los archivos, instala programas que pueden ser maliciosos, controla el sistema de las PC´s por completo.

Cuando un BackDoor´s encuentra ya instalado tiene la capacidad de:

- Crear, eliminar, renombrar, copiar o editar cualquier archivo, ejecutar varios comandos, cambiar cualquier configuración del sistema, alterar el registro de sistema operativo, ejecutar, controlar o acabar con las aplicaciones instaladas.
- Robar información personal sensible, documentos valiosos, contraseñas, nombres, números de tarjetas bancarias e incluso detalles bancarios exactos, actividad del usuario y registros de navegación.
- Grabar pulsaciones de teclado, realizar capturas de pantalla. Además, enviar a todos los datos reunidos a direcciones de email predefinidas, subirlas a servidores de FTP.
- Infectar archivos, corromper aplicaciones instaladas y dañar el sistema completo.

FORMGRABBING

Esta técnica ha estado presente en troyanos bancarios y otras familias de malware por años. El objetivo es recolectar cualquier tipo de información de algún formulario enviado por usuario usando un navegador Web, para lograr esto, el troyano enganchará diferentes llamadas de API, dependiendo del navegador utilizado, interceptará los datos enviados a estas funciones antes de que se transmitan a Internet, es tan fuerte este virus que puede interceptar datos antes de ser encriptados para viajar por canales de HTTPS.

Este virus permite que los botnets recopilen una cantidad impresionante de datos robados, incluidas las credenciales bancarias para todo tipo de servicios en línea. Los datos son almacenados en bases de datos desconocidas que con capaces de almacenarlas e indexarlas de manera eficiente para que la búsqueda de información bancaria sea más específica.

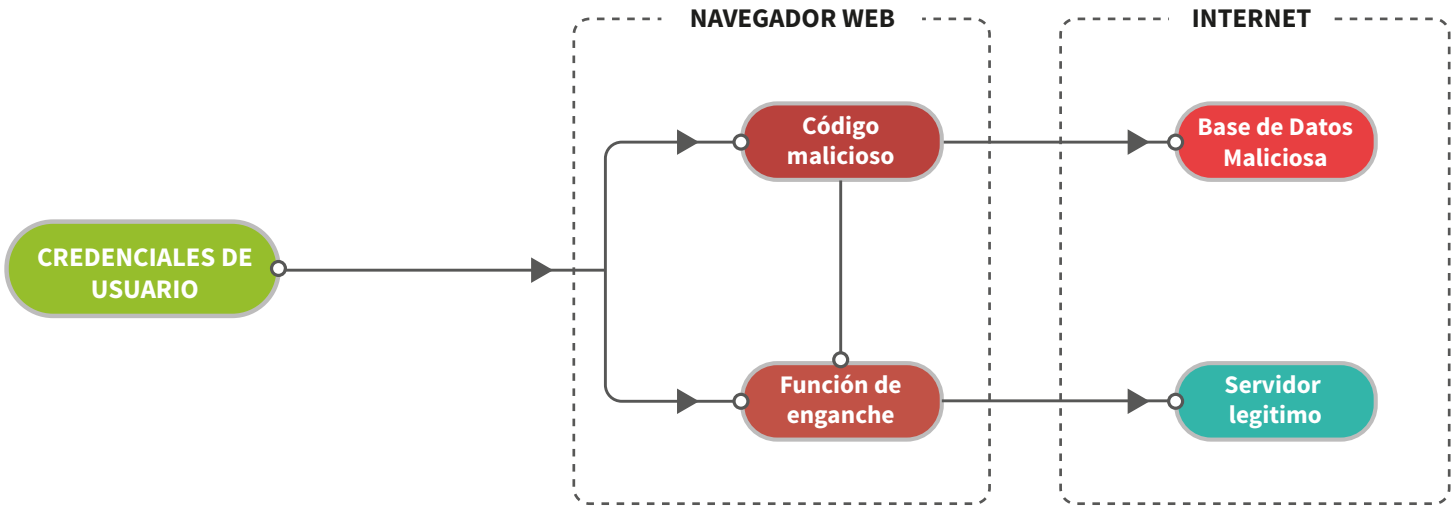


Fig. 3. Uso del API de enganche en un ataque de agarre de formularios

WEBFAKES

Inyecta páginas falsas completas que son réplicas de la página web de la entidad objetivo, diseñadas para engañar a los usuarios para que divulguen información confidencial (como un método de ingeniería social). Estas páginas son tan buenas como las páginas de phishing; sin embargo, llegan directamente a las manos del botmaster.

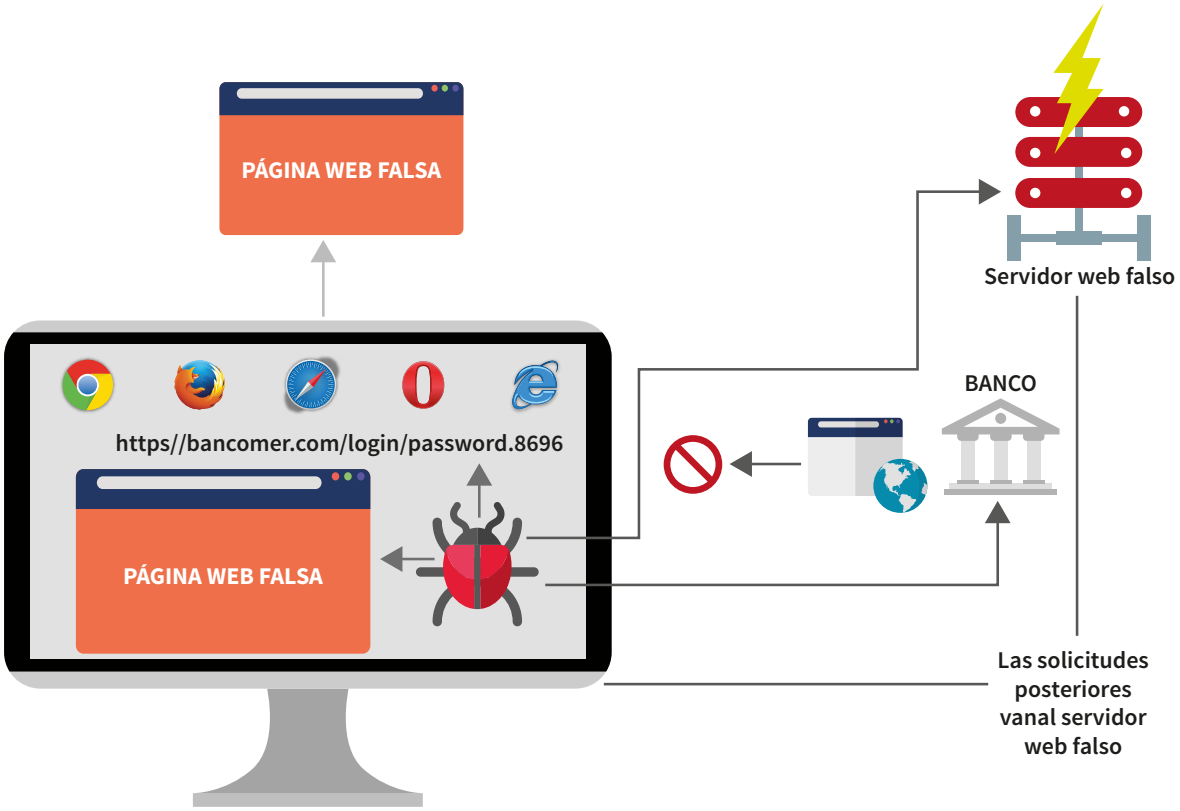


Fig. 4 forma de operar de Webfake

PONY STEALER

Pony Stealer roba contraseñas de aplicaciones comunes como las de mensajería instantánea, los clientes FTP, los navegadores de Internet, los clientes de correo electrónico y las claves de CD de Windows. El malware roba todos los conjuntos de credenciales de formularios de envío, incluidos los utilizados en portales de operaciones bancarias en línea, como parte de su robo de datos de rutina. Pony Stealer también actúa como cargador de otro malware, descargando e implementando troyanos bancarios para facilitar el robo de credenciales bancarias e información de operaciones bancarias en línea. Se suelen encontrar en los mismos servidores C&C en los que está implementada una botnet Zeus.

4. PHISHING

Es una técnica seminal utilizada por los ciberdelincuentes para robar credenciales e información de identificación personal (PII) de sus víctimas. Sigue siendo uno de los vectores de ataque más efectivos, debido al hecho de que normalmente se usa junto con técnicas de ingeniería social para extraer información de sus víctimas.

Los mensajes de phishing parecen provenir de organizaciones legítimas como PayPal, UPS, una agencia gubernamental o su banco. Sin embargo, en realidad se trata de imitaciones. Los correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que hay un problema. Entonces se le redirige a una página web falsa y se le engaña para que facilite información sobre su cuenta, lo que puede provocar el robo de su identidad.

¿Qué tipo de información roba?

- Datos personales
- Información financiera
- Credenciales de acceso

Principales medios de propagación

- Correo electrónico
- Redes sociales
- SMS/MMS
- Llamadas telefónicas
- Infección por malware

Información robada:

- Robo del dinero en la cuenta bancaria.
- Uso indebido de la tarjeta de crédito.
- Estafa.
- Venta de datos personales.

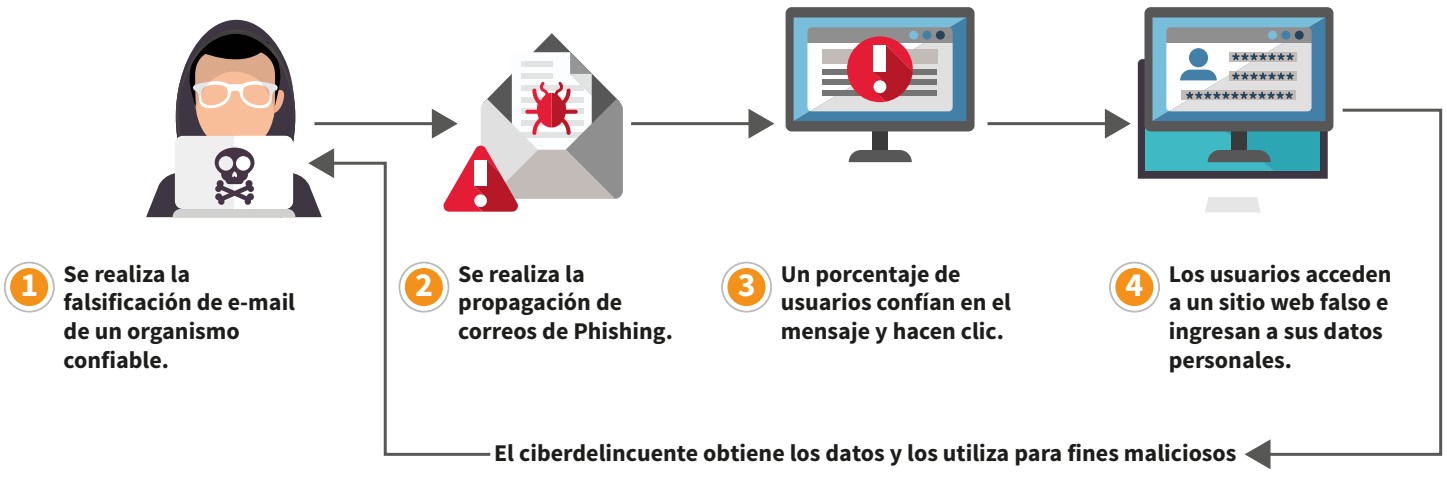


Fig.5 forma de operar del phishing

PHARMING

La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

SPOOFING

Suplantación de la dirección de correo electrónico de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de mensajes de correo electrónico como suplemento perfecto para el uso de suplantación de identidad y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa IP pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Las medidas recomendadas para prevenir estos ataques son crear registros SPF y firmas digitales DKIM.

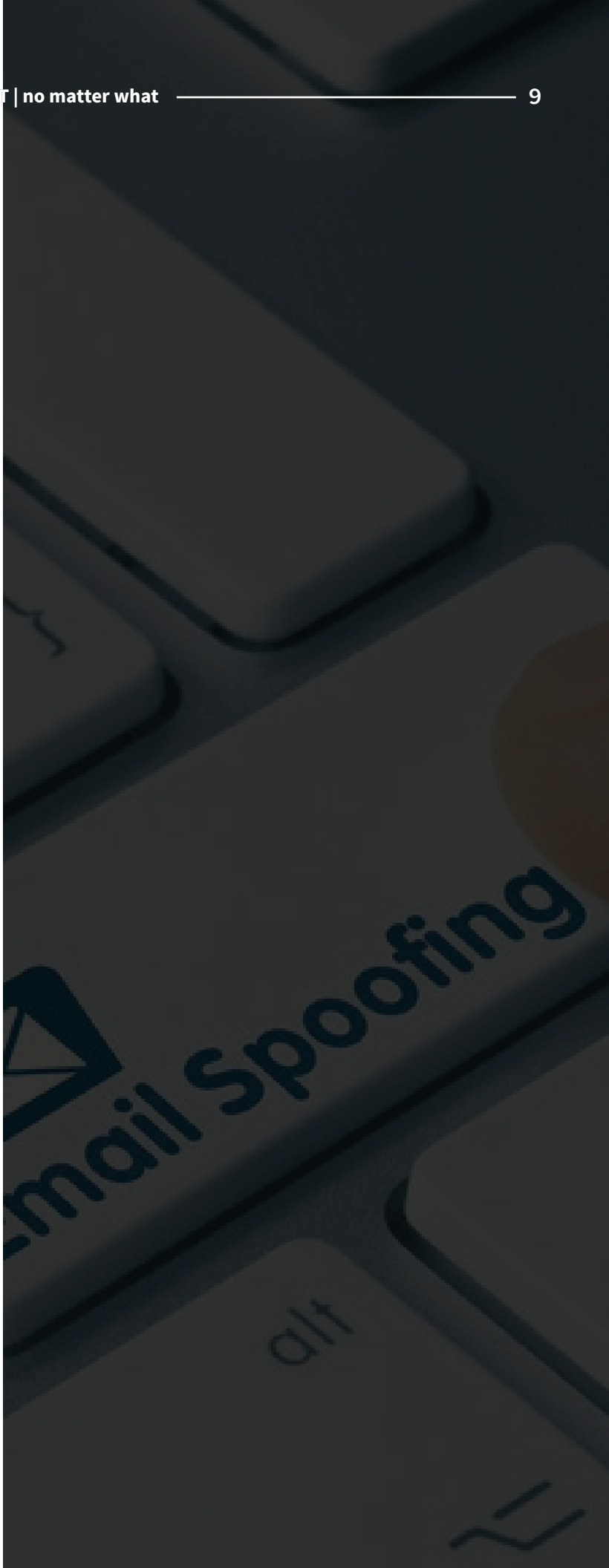
SEARCH ENGINE PHISHING

Los esquemas de Search Engine Phishing pueden venir en una variedad de formas diferentes. Algunos ejemplos comunes de phishing en motores de búsqueda incluyen:

• **Ofertas gratuitas / con descuento:** en este caso, el sitio web puede ofrecer productos a precios muy reducidos, o puede ofrecer artículos gratuitos, que las entidades detrás del sitio web en realidad no poseen y no enviarán. Para obtener los "productos" inexistentes, la persona debe proporcionar su información confidencial.

• **Ofertas de trabajo:** pueden presentarse ofertas de trabajo falsas, que requieren que la persona ingrese su número de seguro social. Estas ofertas pueden surgir en conexión con búsquedas de trabajo en línea.

• **Situaciones de emergencia:** algunos sitios web pueden intentar asustar al consumidor para que proporcione información debido a alguna emergencia o situación urgente. Un ejemplo de esto es un sitio web que establece que la computadora de la persona tiene un virus.



5. MAN IN THE MIDDLE

Es un tipo de ataque cibernético en el que un actor malintencionado se inserta en una conversación entre dos personas, se hace pasar por ambas partes y obtiene acceso a la información que esta siendo transmita por los interesados, esta técnica permite al ciberdelincuente interceptar, enviar y recibir datos destinados a otra persona o usuario, sin que ninguna de las partes lo sepa hasta que ya han sido atacados.

¿Quiénes son susceptibles de ataques?

- Sitios financieros: entre el inicio de sesión y la autenticación
- Conexiones destinadas a ser protegidas por claves públicas o privadas
- Otros sitios que requieres inicios de sesión, donde hay algo que ganar para tener acceso.
- Wifi públicas

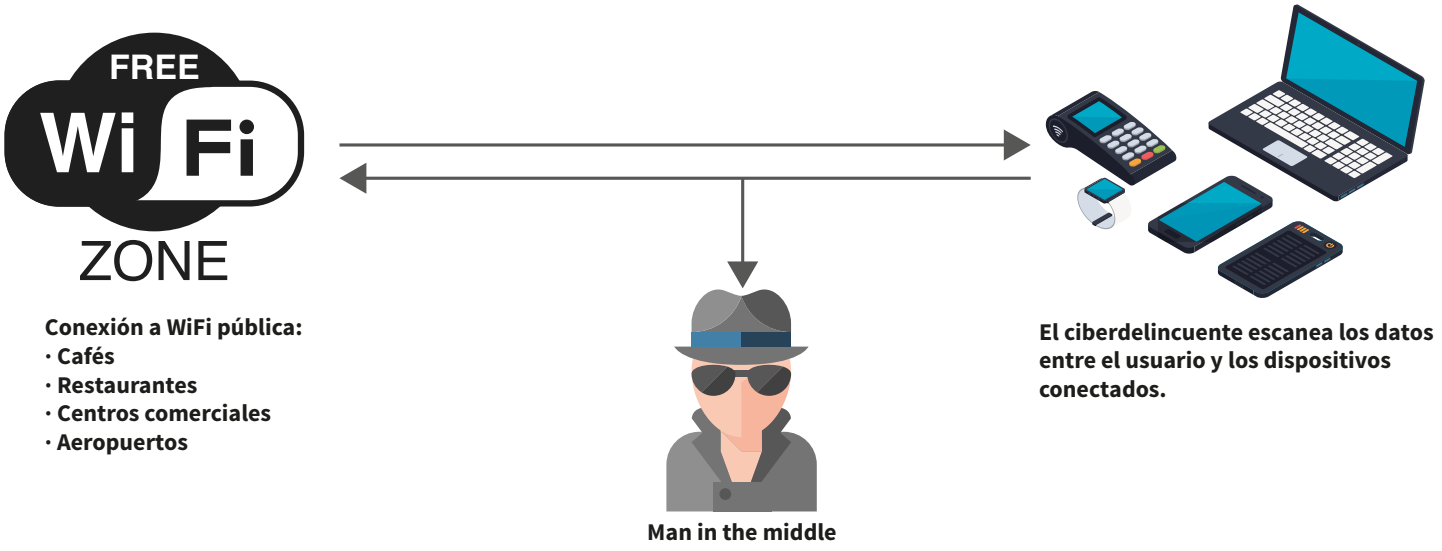


Fig.6 Forma de ataque Man in the middle

6. DNS HIJACKING

El secuestro de DNS o redireccionamiento de DNS es una técnica para alterar la resolución de las consultas del dominio DNS. Esto se puede lograr con un malware que anula la configuración TCP/IP de un equipo para que se redireccione a un servidor DNS falso bajo el control de un ciberdelincuente.

En el DNS Hijacking, un dominio es tomado ilegalmente del propietario legítimo. Su forma más agresiva es el robo de dominios. Estos estafadores a menudo tienen acceso al registro de dominios a través del robo de identidad. El secuestrador asume la identidad del propietario legítimo y modifica la información del registro para reasignar el dominio a sí mismo y así robarlo. Algunos servicios de registro actúan con rapidez cuando se detecta un fraude de este tipo. Sin embargo, también ocurre que sólo se toman medidas cuando se aplican por ley. En algunos casos, el hijacker puede mantener el control del dominio. En la mayoría de los casos, las víctimas no tienen la voluntad ni los medios financieros para llevar a cabo procedimientos judiciales largos y lentos que les devolverían el dominio. El hecho de que los secuestradores actúen en otro país también es un factor disuasorio. Mientras tanto, el secuestrador tiene control total sobre el dominio y puede disponer libremente del contenido o redirigir los códigos de estado HTTP.

Algunos ataques de secuestro de DNS comunes incluyen:

- Las estafas de suplantación de identidad (phishing) en las que el sitio de destino se reemplaza por un sitio web completamente diferente que se ve y actúa como el original.
- Sitios de rastreo de datos que imitan a los sitios de banca o de compras en línea e intentan obtener detalles de inicio de sesión.
- El llamado secuestro "suave" donde un ISP redirige el tráfico para obtener ingresos por publicidad. Estas pueden ser redirecciones inocentes en el caso de URL mal escritas, o pueden ser maliciosas.
- Suplantación de DNS por parte de los gobiernos para censurar los datos mediante el bloqueo o la redirección de las solicitudes de DNS.

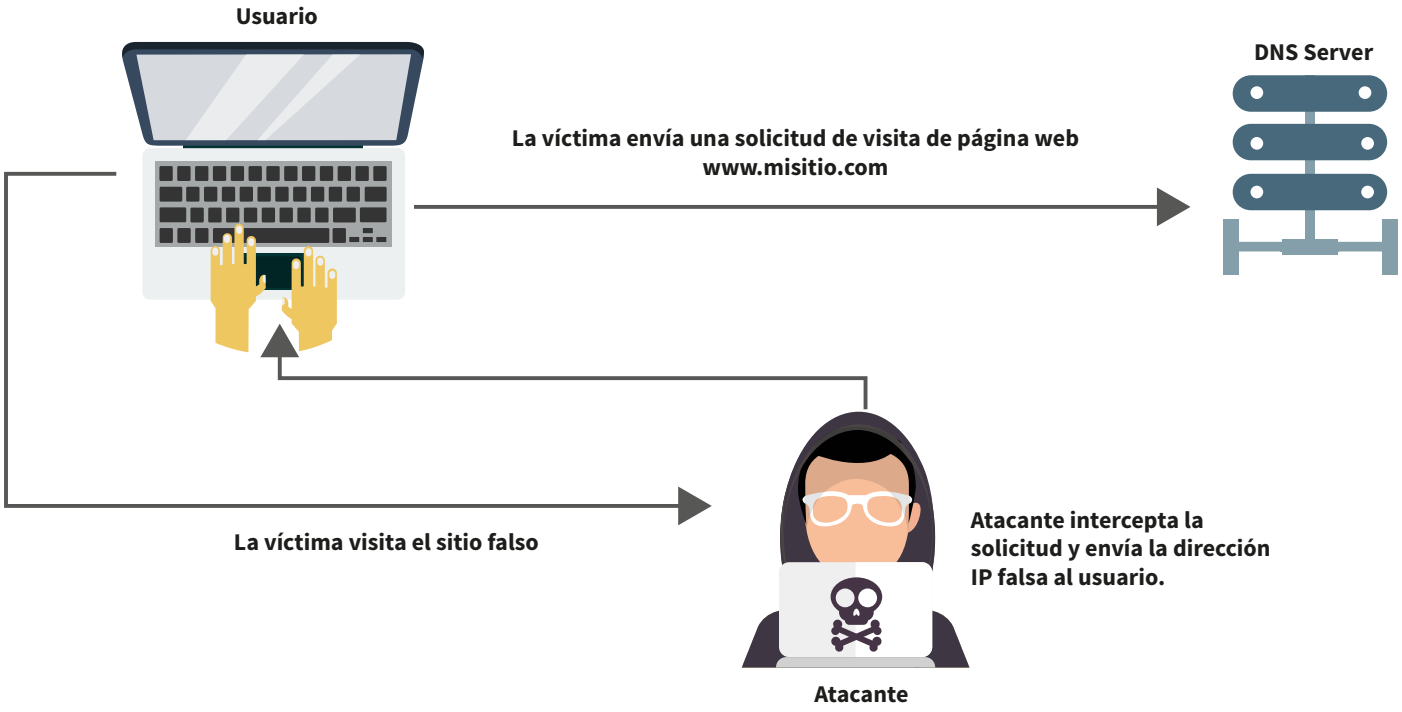


Fig 7 Forma de ataque DNS Hijacking

7. ATAQUE DE FUERZA BRUTA

Existen dos tipos de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Destributed Denial of Service). La diferencia entre ambos es el número de equipos o IP´s que realizan el ataque.

En el ataque DoS se genera una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se logra la denegación del servicio.

En el taque DDoS se generan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio que se desea sea objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones proviene desde diferentes IP´s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

Los equipos donde se realizan los ataques DDoS son infectados por medio de algún malware, para después convertirse en bots o zombis, y estos son controlados de forma remota por un ciberdelincuente. Un conjunto de ordenadores (bots) infectados por el mismo malware, forman una botnet o también conocida como red zombi. Esta red tiene mayor capacidad para derribar servidores que un ataque realizado por sólo una máquina

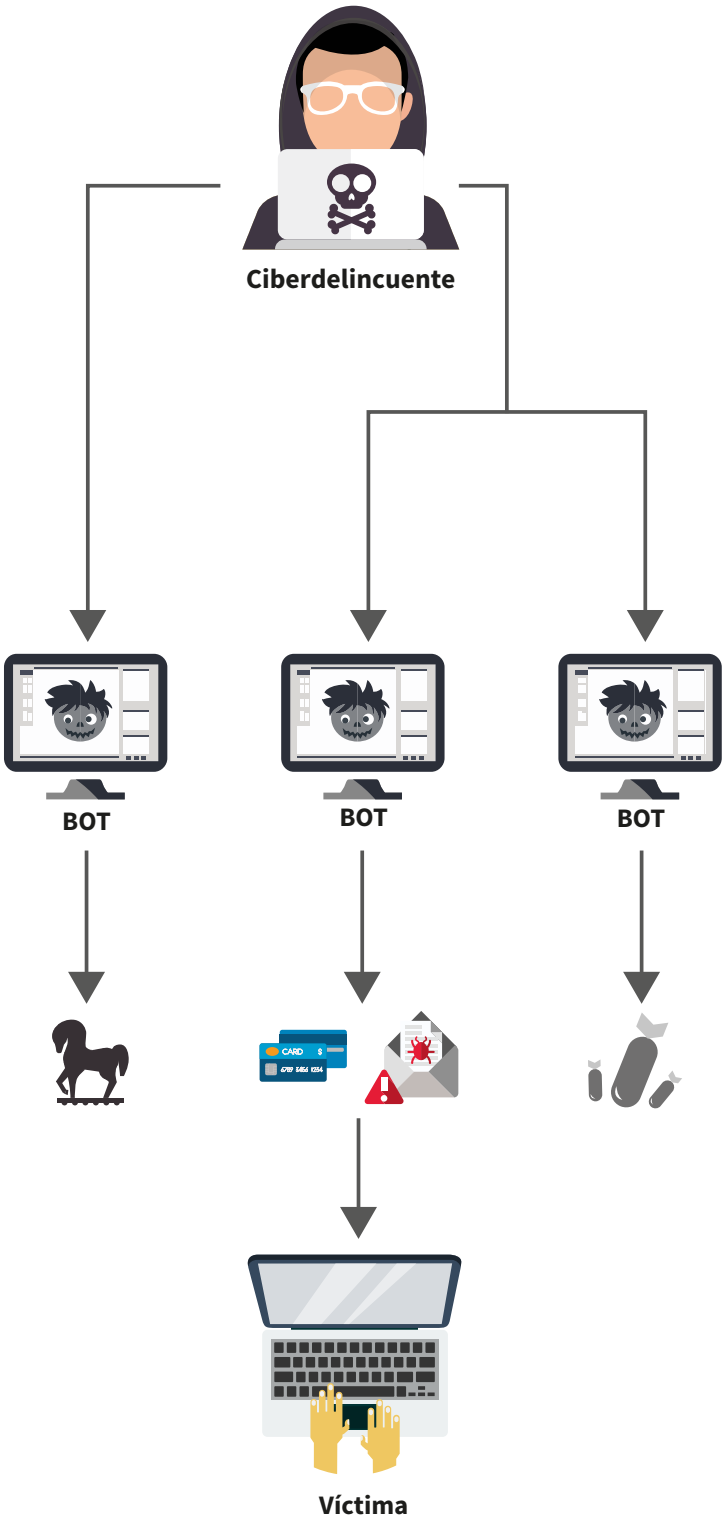
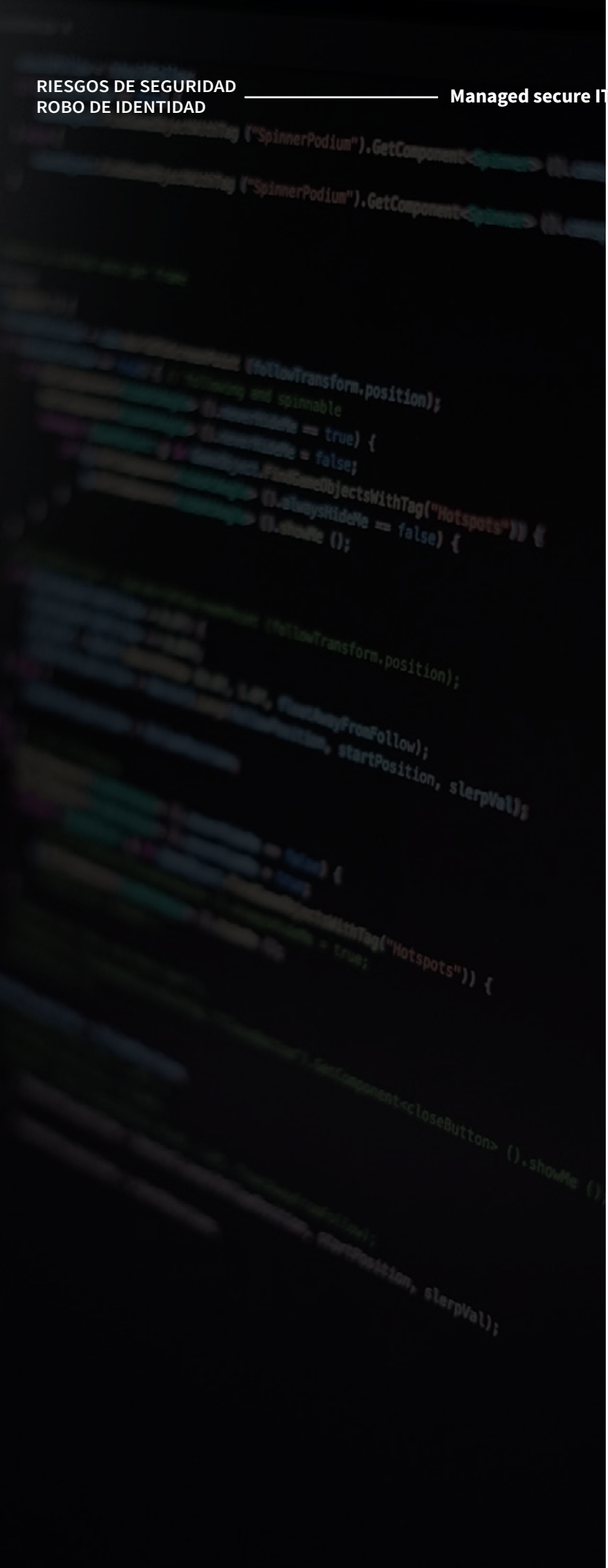


Fig. 7 Forma de ataque DDOs



ATAQUE DE DICCIONARIO

El ataque por diccionario es un tipo de ataque que utiliza un diccionario de palabras para llevar a cabo el robo de contraseñas.

¿Cómo funciona?, para ingresar a un sistema con contraseña, se puede utilizar un diccionario con palabras frecuentes y un programa automáticamente irá probando una a una para descifrarla.

Este tipo de ataque tiende a funcionar debido a que muchas personas emplean claves sencillas, incluso palabras del diccionario, tal vez apenas combinadas con uno o dos números.

TABLAS ARCOÍRIS

Parten del valor hash para reproducir los pasos de la cadena hasta obtener la contraseña. Muchas veces el valor no se encuentra en la tabla; por lo que se recrea al reducir el valor con la misma función con la cual se creó la cadena.

Este procedimiento se repite hasta conseguir el valor. Esto no significa que se ha encontrado la contraseña, sino la cadena de caracteres que al final terminará revelando el texto plano que compone la contraseña.

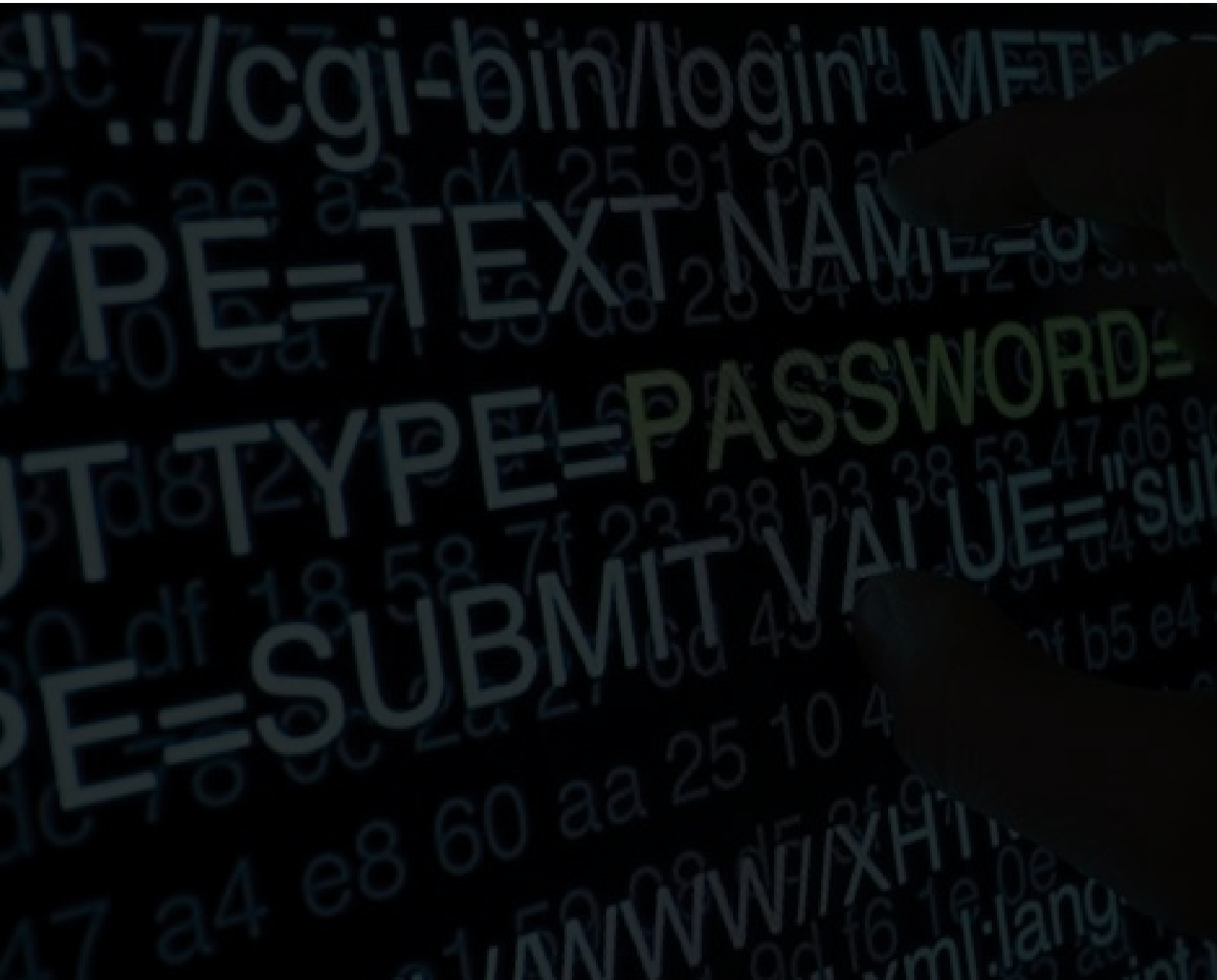
Se les llaman Tablas Arcoíris porque se asigna un color distinto a cada reducción para evitar confusiones. Al final son tantas las reducciones con sus respectivos colores, que termina por parecer un arcoíris.

¿SE PUEDEN UTILIZAR ESTOS TRES ATAQUES SIMULTÁNEAMENTE?

La respuesta es: sí. La estrategia de ataque de diccionario (centrada en detección de palabras); y la de las tablas arcoíris (que emplea grupos de secuencias contiguas) pueden complementar los ataques de fuerza bruta; y hacer que las recomendaciones básicas para la creación de contraseñas resulten insuficientes.

Esto ocurre especialmente cuando creamos contraseñas en la web, porque estamos sujetos a lo que el proveedor del servicio disponga. Sobre todo, por que usualmente se establecen parámetros de máximo 10 caracteres; además de un número limitado de números y caracteres que vuelven más vulnerable nuestras contraseñas. Un ciberdelincuente puede perfectamente ajustar su software con estas características para acelerar el proceso de ruptura de código.

Sin embargo, los servicios online disponen de dos factores que pueden ayudar a combatir los ataques de fuerza bruta por sí mismos o en combinación con las otras dos modalidades antes descritas.



8. VULNERABILIDADES

DESARROLLO SEGURO RIESGOS DE SEGURIDAD DE APLICACIONES

INYECCIÓN:

Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización

PERDIDA DE AUTENTICACIÓN:

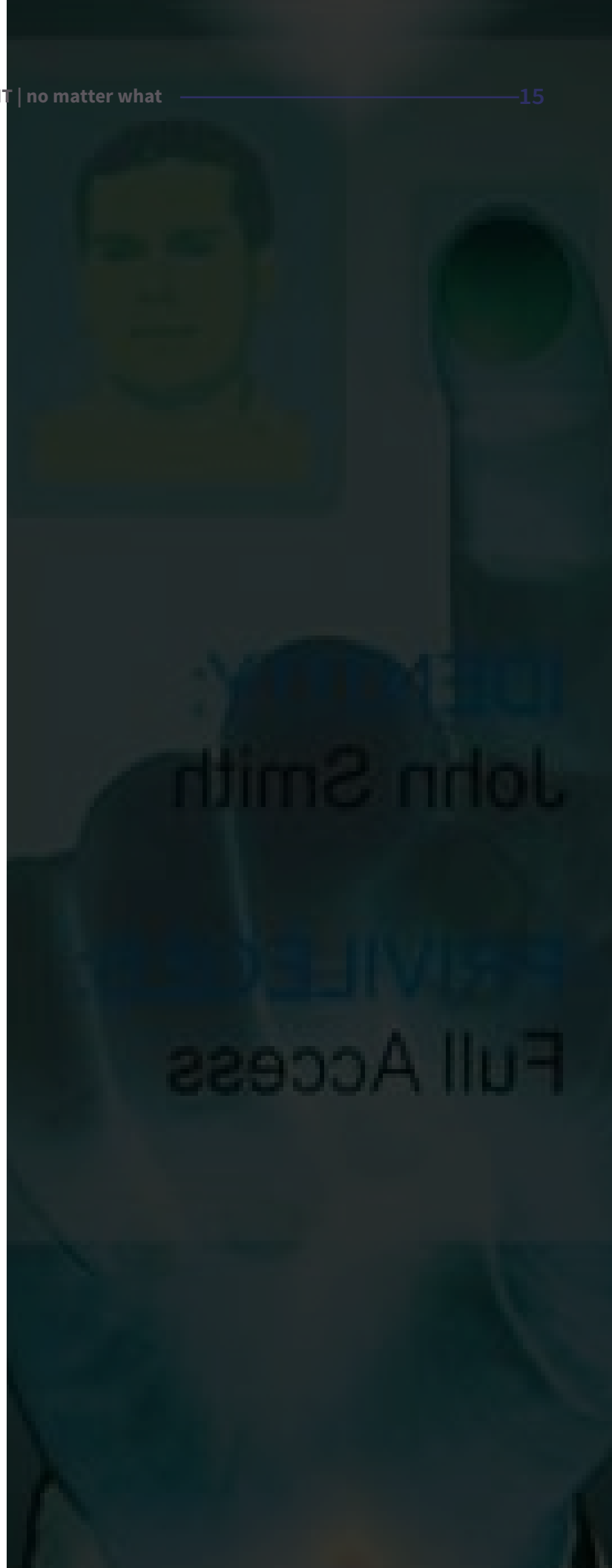
Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los ciberdelincuentes comprometer los usuarios y contraseñas, token de sesiones o explotar otras fallas de implementación para robar la identidad de otros usuarios ya sea de forma temporal o permanente.

EXPOSICIÓN DE DATOS SENSIBLES:

Muchas aplicaciones WEB y API´s no protegen adecuadamente los datos sensibles, tales como información financiera, de salud o información que hace una a una persona identificable los ciberdelincuentes pueden robar o modificar estos datos protegido de forma inadecuada para llevar a cabo fraudes con tarjetas de crédito/debito, robos de identidad u otros delitos. Los datos sensibles requieres métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

PERDIDA DE CONTROL DE ACCESO

Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos. Cambiar derechas de accesos y permisos.



SECUENCIA DE COMANDOS EN SITIOS CRUZADOS (XSS)

Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador WEB sin una validación y codificación apropiada, o actualiza una pagina web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar los sitios web o redireccionar al usuario hacia un sitio malicioso. Ciclo de vida de la aplicación de acuerdo a los requerimientos de seguridad de la información.

GENERACIÓN DE REQUISITOS DEL NEGOCIO Y LOS RECURSOS:

1. Recolectar y negociar los requisitos del negocio para el diseño y elaboración de una aplicación, incluyendo la confidencialidad, autenticidad, integridad y disponibilidad de todos los activos de datos y de las funciones del negocio.

2. Recopilar los requerimientos técnicos incluyendo los requerimientos de seguridad de la información funcionarles y no funcionales.

3. Planear y negociar de acuerdo con el presupuesto si se cubren todos los aspectos del diseño, construcción, pruebas y puesta en producción y asegurar que estas etapas incluyan los requisitos de seguridad de la información.

GENERACIÓN DEL DOCUMENTO DE ALCANCE

1. Solicitar a los desarrolladores internos/externos que se incluyan los requisitos de seguridad de la información de acuerdo a los estándares existentes como puede ser OWASP para desarrollos seguros.

2. Evaluar el cumplimiento de todos los requerimientos técnicos, incluyendo las fases de planificación y diseño de la aplicación.

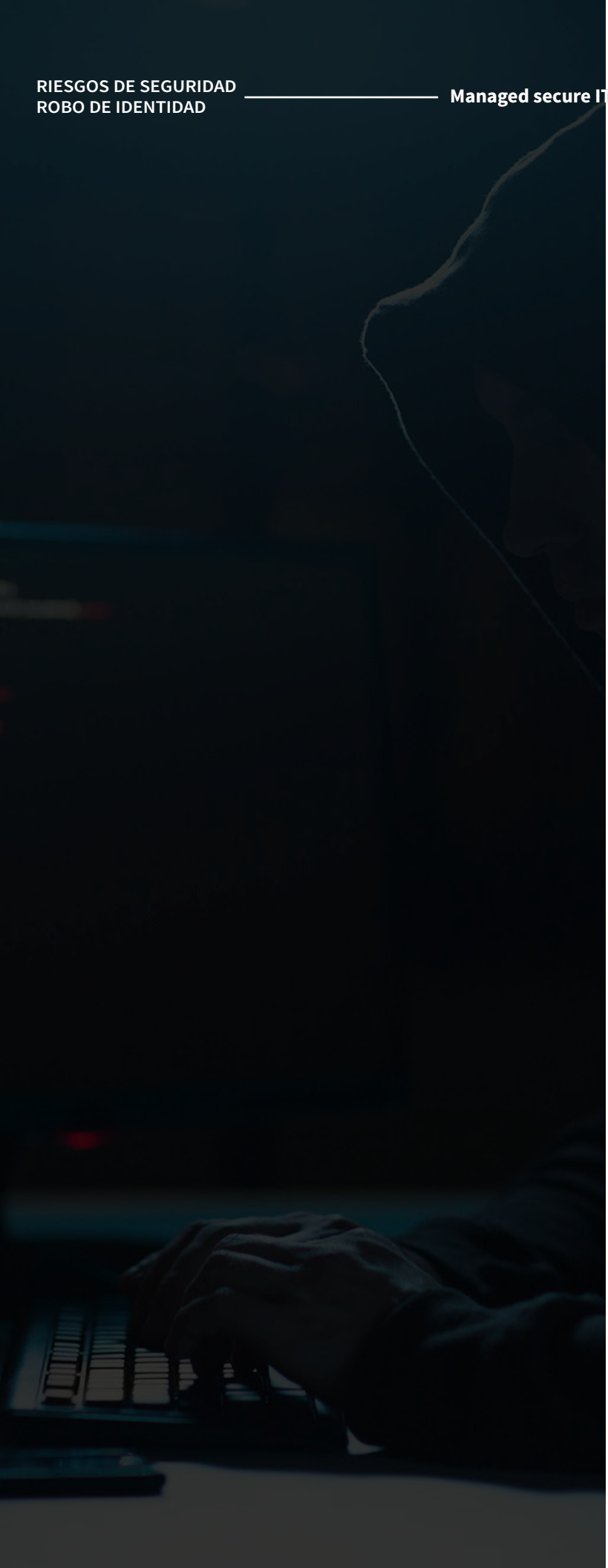
3. Negociar todos lo requerimientos técnicos incluyendo el diseño, seguridad y acuerdo de niveles de servicio durante todo el proyecto.

PLANIFICACIÓN Y DISEÑO

1. Definir la arquitectura de seguridad de la información, controles y contramedidas adecuadas a las necesidades de protección y el nivel de amenazas planificado. Esto debería contar con el apoyo de especialistas en seguridad.

2. Asegurar que el propietario de la aplicación acepta los riesgos residuales o bien que se tengan los recursos necesarios para las remediaciones.

3. En cada etapa del proyecto, asegurar que se crean los casos de uso para validar los requisitos de seguridad de la información y restricciones para requerimientos no funcionales.



PRUEBAS Y PUESTA EN PRODUCCIÓN:

1. Automatizar el despliegue seguro de la aplicación, interfaces y todo componente, incluyendo las autorizaciones requeridas.

2. Probar las funciones técnicas, integración a la arquitectura de TI, y coordinar pruebas de funciones de negocio.

3. Crear casos de “uso” y de “abuso” tanto desde el punto de vista netamente técnico como del negocio.

4. Administrar pruebas de seguridad de la información de acuerdo a los procesos internos, las necesidades de protección y el nivel de amenazas asumido para la aplicación.

5. Poner la aplicación en operación y migrar las aplicaciones usadas previamente en caso de ser necesario.

6. Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad (CMDB) y la arquitectura de seguridad.

OPERACIÓN:

1. Operar incluyendo la administración de seguridad de la aplicación (por ej. administración de parches).

2. Aumentar la conciencia de seguridad de los usuarios y administrar conflictos de usabilidad vs seguridad.

3. Panificar y gestionar cambios, por ejemplo, la migración a nuevas versiones de la aplicación u otros componentes como sistema operativo, interfaces de software y bibliotecas.

4. Actualizar toda la documentación, incluyendo la Base de Datos de Gestión de la Seguridad (CMDB) y la arquitectura de seguridad.

BAJA DE APLICACIÓN

1. Cualquier dato requerido debe ser almacenado. Otros datos deben ser eliminados de forma segura.

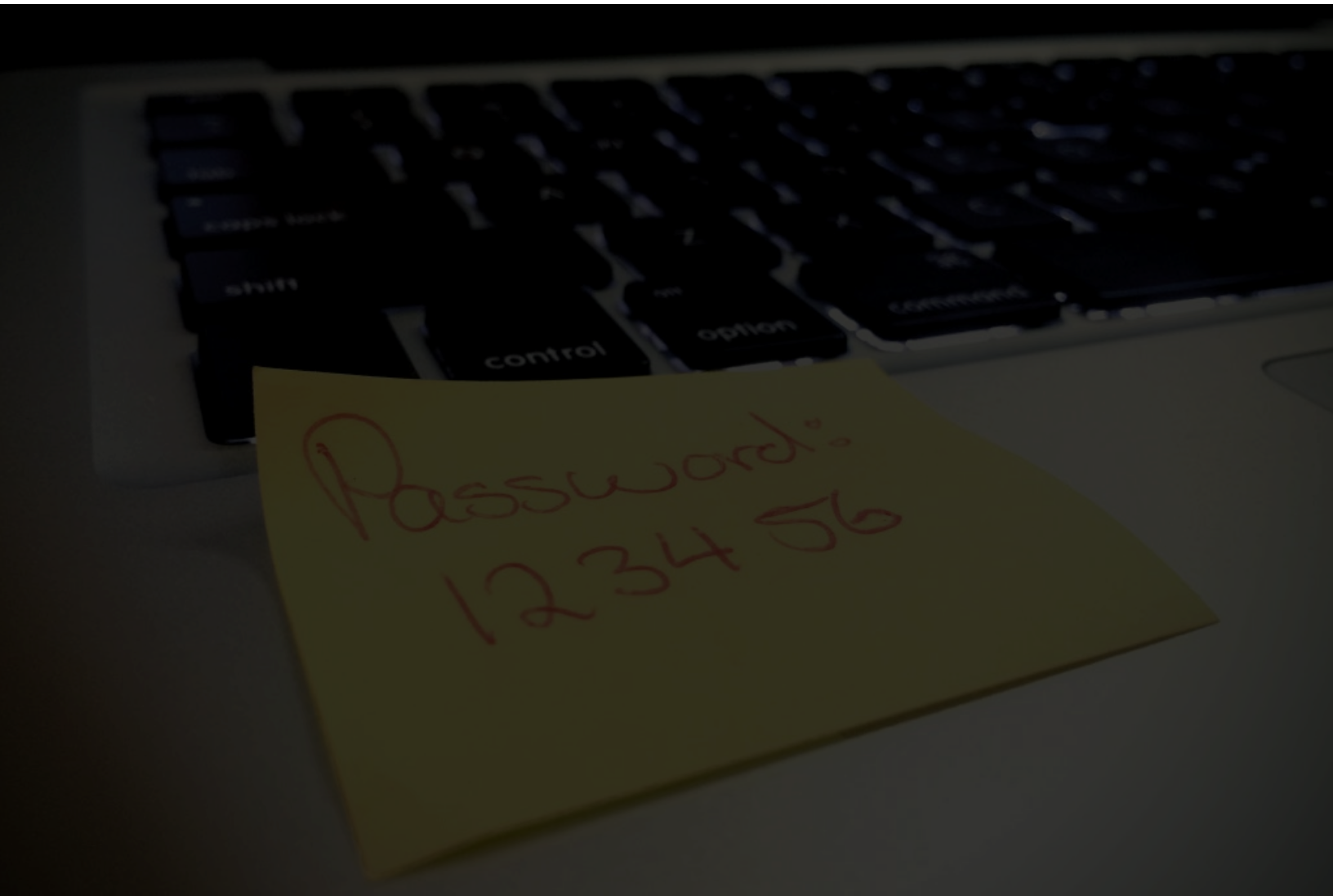
2. Retirar la aplicación en forma segura, incluyendo el borrado de cuentas, roles y permisos no usados.

3. Establecer el estado de la aplicación a “baja de aplicativo” en la CMDB.

9. NO TÉCNICAS

Hay una serie de otros métodos no técnicos que exponen las credenciales. Por ejemplo, el "surfeo de hombro" de extraños o estar lo suficientemente cerca como para observar una transacción financiera, sigue siendo un problema bastante extendido. Aún más básico es simplemente compartir contraseñas y otras credenciales con otros en el mundo físico, como en un post-it o similar. Los dispositivos móviles están especialmente en riesgo, ya que los usuarios a menudo realizan transacciones confidenciales en lugares públicos, ¡Nunca se sabe quién está mirando! Además, se han sucitado casos de piratas informáticos dirigidos a cámaras de seguridad que pasan por alto ciertas áreas de actividad sensible, como cajeros automáticos, puntos WiFi-públicos, etc. Los atacantes pueden robar credenciales al observar las imágenes robadas de las cámaras de circuito cerrado.

La ingeniería social es la manipulación psicológica de las víctimas y, en general, es una técnica no técnica mediante la cual los malos cosechan las credenciales. Se basa en la interacción humana y engaña a las personas para que rompan los protocolos de seguridad que suelen cumplir. Por ejemplo, los atacantes pueden intentar engañar a las víctimas para que ofrezcan acceso a información confidencial a través de llamadas telefónicas, redes sociales e incluso reunirse con empleados de la compañía en persona. Este tipo de técnica, cuando se realiza sin automatización o actividad digital, generalmente se realiza en ataques dirigidos.



EL ROBO DE IDENTIDAD SUELE SER UTILIZADA PARA:

FRAUDE

Se pueden realizar diferentes tipos de fraude cuando se toma una cuenta, desde transferencias y compras, hasta lavado de dinero y estafas de seguros. En algunos casos específicos, la cuenta se puede utilizar para realizar acciones fraudulentas, como los siguientes perfiles en las redes sociales.

VENTA DE INFORMACIÓN

Tener acceso a cuentas robadas o datos violados significa tener acceso a información personal valiosa (PII) para ser vendida en mercados clandestinos. En algunos casos, después de una violación de datos a gran escala, las credenciales y la información de la tarjeta de crédito también se pueden vender en lotes en tiendas subterráneas específicas, a menudo controladas por los mismos atacantes.

CHANTAJE

Otra consecuencia importante de las adquisiciones de cuentas es el chantaje. Con el acceso a cuentas o sistemas, la información confidencial no se vende, sino que se redirige a los legítimos propietarios.

CRIMEWARE

Los ciberdelincuentes utilizan principalmente el correo electrónico, el sistema y las credenciales de las redes sociales para distribuir malware, realizar campañas de phishing o infectar sitios web para agregar contenido malicioso.

DAÑO REPUTACIONAL

Este puede ser el objetivo principal de un ciberdelincuente o competidor, que usara el acceso a la cuenta robada para dañar la imagen de una persona o compañía. También es una consecuencia secundaria de algunos otros objetivos criminales como el crimeware o el hacktivismo.

HACKTIVISMO

Los hacktivistas pueden realizar desconfiguraciones, exponer controversias de las compañías o hacerse pasar por personas conocidas en las redes sociales. Esto también puede tener un impacto de reputación secundaria.

ESPIONAJE

Las cuentas robadas son utilizadas para espiar y recopilar información de los propietarios, va desde las operaciones individuales hasta los movimientos corporativos inclusive actividades a niveles de estados nacionales. El espionaje de los estados nacionales puede impactar directamente en las negociaciones políticas y las estrategias de un país.

10. Conclusiones

La educación para el recurso humanos es la clave para poder mitigar los ataques. Es importante analizar si al día de hoy su organización de encuentra preparada para poder identificar y mitigar ataques, por ejemplo: saber identificar un correo phishing. Es importante que las organizaciones reconozcan y lleven a cabo actividades de entrenamiento para todo su personal, ya que no solo el contar con un área o responsable de seguridad de la información es suficiente. La capacidad de no reconocer cuando se esta bajo un ataque podría comprometer gravemente a la organización con el entrenamiento adecuado se puede ahorrar una gran cantidad preocupación y pérdida económica.

Otro aspecto muy importante es el poder conocer como nos podemos proteger de forma individual y así poder llevar este conocimiento a los familiares ya que al día de hoy la educación en materia de seguridad de la información no es de conocimiento de todas las personas.

Cifras de la CONDUSEF nos muestra que:
• México ocupa el 8° lugar a nivel mundial en el delito de robo de identidad
• El 67% es por perdida de documentos
• El 63% es por robo de cartera o portafolio
• El 53% es por información tomada de una cuenta bancaria

Algunas recomendaciones:
• No ingreses nombres de usuario y contraseñas en sitios desconocidos.
• Evita compartir información financiera.
• Utiliza sólo páginas electrónicas que cuenten con certificados de seguridad.
• En caso de extravío de documentos personales presenta una denuncia ante la autoridad correspondiente.
• Evita proporcionar datos personales a encuestadores vía telefónica.
• Revisa periódicamente tus estados de cuenta para detectar a tiempo cualquier operación irregular.

¿Cómo pueden robar tu identidad?
• Si no tomas las debidas precauciones al realizar compras, pagos de servicios, de impuestos o transacciones bancarias vía internet.
• Robo de teléfonos celulares.
• Si proporcionas demasiada información a través de redes sociales.
• En estados de cuenta o documentos personales que tiras sin precaución a la basura.
• Robo de correspondencia.
• Robo de carteras o bolsos con tarjetas de crédito e identificaciones.

¿Qué hacer en caso de robo de identidad?
• Contacta a tu Institución Financiera para solicitar la cancelación de tus tarjetas y la emisión de una "alerta de fraude".
• Cambia las contraseñas o bloquea las cuentas que pudieran estar comprometidas.
• Algunas de las entidades que te pueden apoyar son: Condusef, PROFECO y la Policía Federal.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.