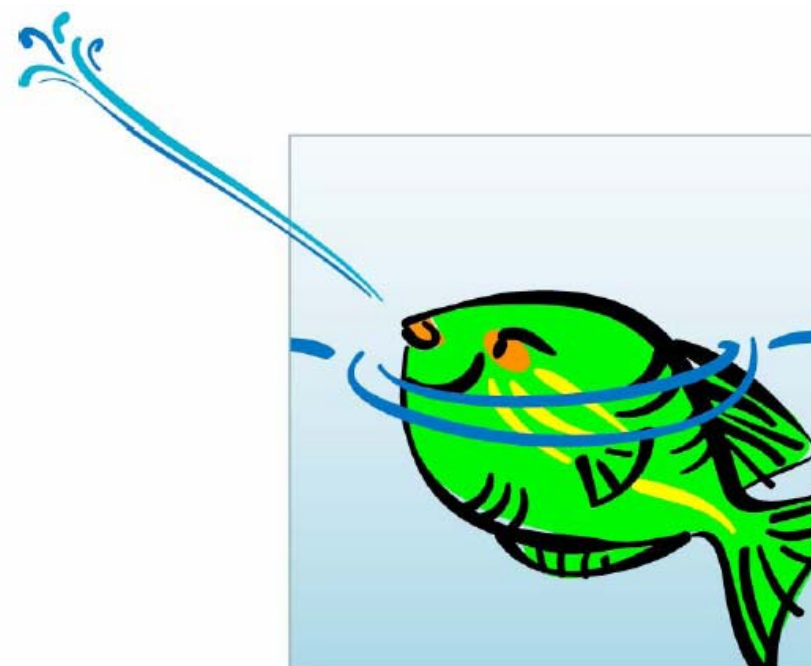


Las profundidades del Phishing

Gonzalo Álvarez Marañón

Qué

- ❑ De pesca en Internet
 - ❑ Qué es el Phishing
- ❑ Lección de biología
 - ❑ Ciclo de vida del Phishing
- ❑ Guía para naturalistas
 - ❑ Taxonomía de tipos de Phishing
- ❑ Vedado de pesca
 - ❑ Soluciones contra el Phishing



Qué es el Phishing

- ❑ Nueva forma de **fraude**
- ❑ Se basa en la picaresca (ingeniería social)
- ❑ Objetivo: Robo de identidad digital
- ❑ Impacto:
 - ❑ Pérdidas directas: dinero robado, emisión de nuevas tarjetas, soporte telefónico, gastos judiciales
 - ❑ Pérdidas indirectas motivadas por la erosión de la confianza: vuelta a canales tradicionales de comunicación, daño a la imagen, pérdida de clientes
 - ❑ Amenaza a las relaciones a través del canal electrónico

Si hoy mismo recibiera un mensaje legítimo de correo de su banco, ¿confiaría en él?

Qué es el Phishing

- ❑ Un atacante (el phisher) se hace pasar por una compañía o institución financiera de reconocido prestigio
- ❑ Envía mensajes de forma masiva (el primer cebo), habitualmente a través del correo electrónico, aunque podrían utilizarse otros canales
- ❑ Los mensajes están dirigidos a potenciales clientes (phish, el pescado) de la organización suplantada
- ❑ Si muerden el anzuelo son redirigidos a un sitio web idéntico al original (el segundo cebo)
- ❑ Recolecta la información personal
- ❑ Una vez robada la identidad de la víctima, el atacante podrá suplantarla ante el servicio legítimo

Problema de autenticación

5% de los clientes alcanzados pican

2,5 millones de mensajes en un día

1ª suplantación: el mensaje

- ❑ Necesidad de convicción
 - ❑ Aspecto oficial: imagen, lenguaje, tono
 - ❑ Cebo apetitoso para incitar al clic
 - ❑ Problema gravísimo de resolución urgente
 - ❑ Nuevos servicios u ofertas con grandes ventajas
 - ❑ Necesidad de renovar un servicio o cuenta
 - ❑ Inclusión de datos personales (spear phishing)
 - ❑ Regalo, premio o promoción
 - ❑ Ayuda humanitaria para víctimas del desastre X
- ❑ Kits de phishing
 - ❑ Incluyen plantillas para mensajes de correo y para web
 - ❑ Listas de destinatarios
 - ❑ Técnicas de blanqueo de dinero

2ª suplantación: el sitio web

- ❑ Necesidad de convicción
 - ❑ Copia idéntica del sitio suplantado
 - ❑ Detalles más complicados
 - ❑ Falsificación del URL
 - ❑ Falsificación de otros elementos del navegador
 - Candadito
 - Barra de estado
 - Información de certificados

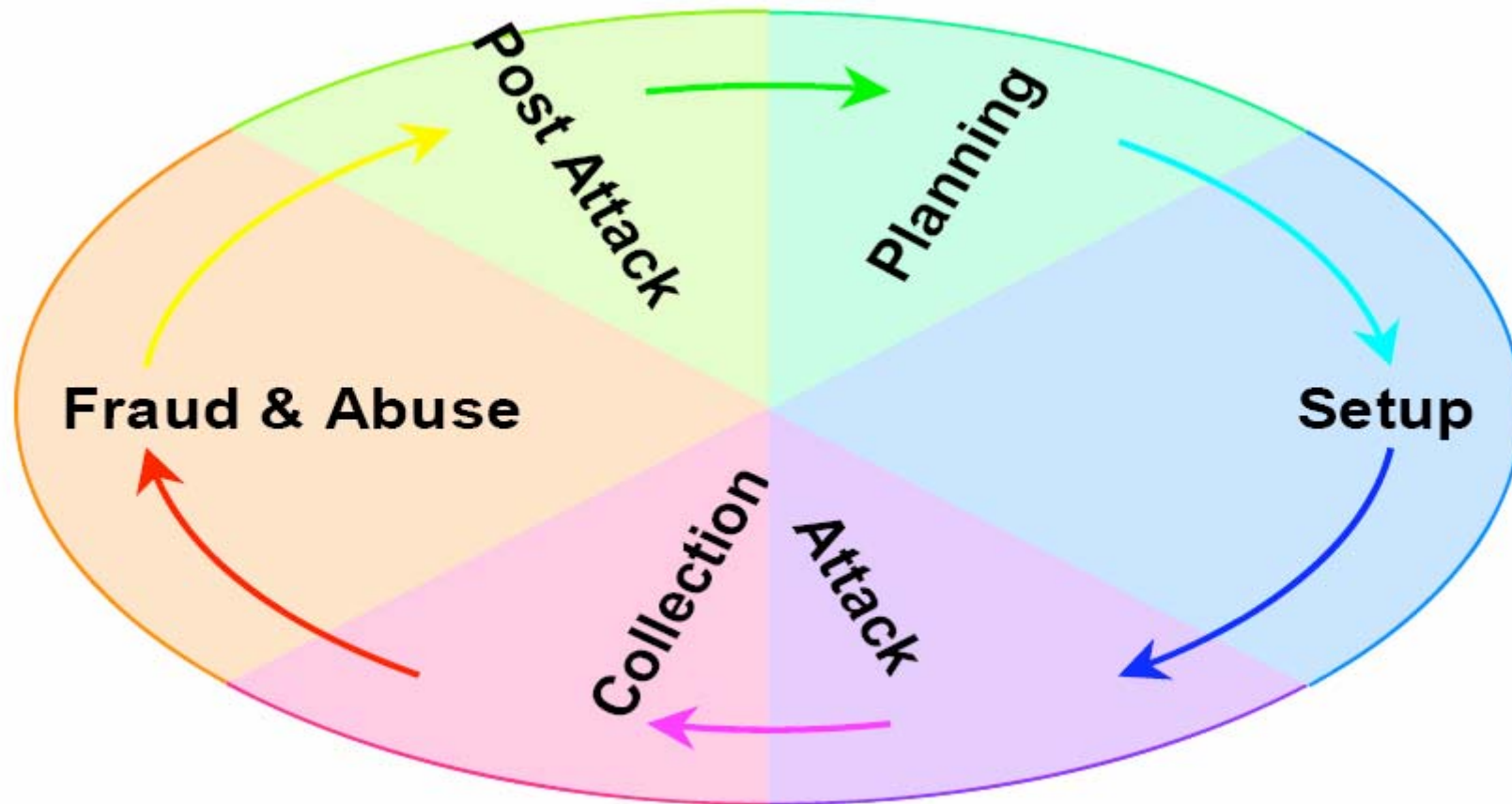


3ª suplantación: el cliente

- ❑ Presentar la información personal robada
 - ❑ Nombre de usuario y contraseña: la más fácil
 - ❑ Falsificación de tarjetas para cajeros
 - ❑ Por desgracia, los bancos hacen poco o nada por mejorar sus débiles mecanismos de autenticación



Ciclo de vida del Phishing



Planificación

- ❑ Determinación del objetivo
 - ❑ La entidad a atacar: banco, comercio
 - ❑ Las víctimas potenciales: los clientes
 - ❑ La información personal a robar: credenciales, números de tarjeta, de seguridad social
- ❑ Determinación de la finalidad del ataque
 - ❑ Venta, explotación, chantaje
- ❑ Determinación del canal de comunicaciones
 - ❑ Correo electrónico, mensajería instantánea, chat, anuncios en páginas web, troyanos

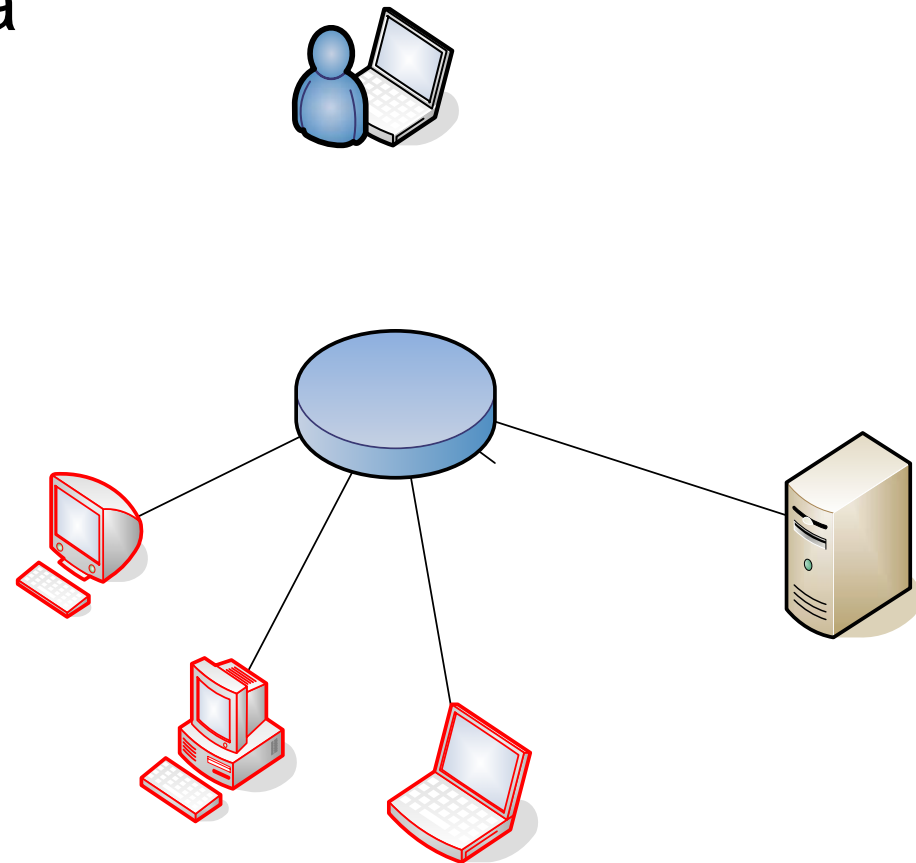
Preparación

- ❑ Creación de los materiales necesarios
 - ❑ Plantilla para el mensaje
 - ❑ Base de datos de destinatarios
 - ❑ Botnet para enviar los mensajes
 - ❑ Sitio web para recolectar los datos



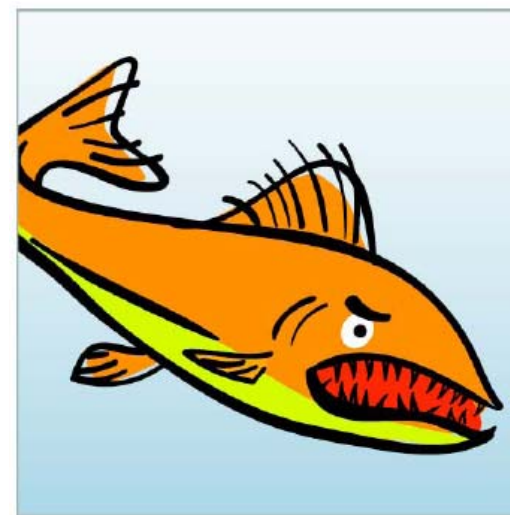
Ataque

- ❑ Puesta en marcha de la infraestructura de ataque
 - ❑ Control de la botnet a través del IRC
 - ❑ Los zombies envían los mensajes a la lista



Recolección

- ❑ Recolección de la información personal
 - ❑ Correo electrónico en cuentas anónimas
 - ❑ Envío al canal de chat del bot
 - ❑ Volcado en la BD del sitio web y consulta a través del navegador
 - ❑ ...



Fraude

- ❑ Normalmente, el phisher no explota la información, la vende a cashers
- ❑ Mercado de phishing
 - ❑ 0,50 € número de tarjeta válido
 - ❑ 100,00 € cuenta bancaria completa
 - ❑ Número
 - ❑ Saldo
 - ❑ Tarjetas: número, caducidad, cvv2, PIN

Blanqueo de dinero

- ❑ Reclutamiento de muleros
 - ❑ Scam: Ofertas de trabajo desde casa en bolsas online de trabajo, spam, spim
 - ❑ Crean cuenta bancaria donde reciben transferencias desde las cuentas atacadas
 - ❑ Envían el dinero al extranjero a cambio de una comisión
 - ❑ La policía detiene al mulero, no al casher

Blanqueo de dinero

- ❑ Fraude en cajeros
 - ❑ Grabación de tarjetas de banda magnética
 - ❑ Algoritmo de volcado de la información débiles (los bancos más demandados) y fuertes
 - ❑ Retirada del máximo permitido diario

Curiosidad

❑ Fraude en cajeros



Curiosidad

❑ Fraude en cajeros



Blanqueo de dinero

- ❑ Cuentas bancarias sin fondos
 - ❑ Utilizadas como puentes para cadenas de transferencias
- ❑ Otras entidades
 - ❑ Comercios electrónicos, especialmente de venta de bienes digitales: música, software
 - ❑ PayPal
 - ❑ eBay
 - ❑ Cuentas en proveedores de acceso a Internet
 - ❑ Llamadas telefónicas desde Internet (Skype)

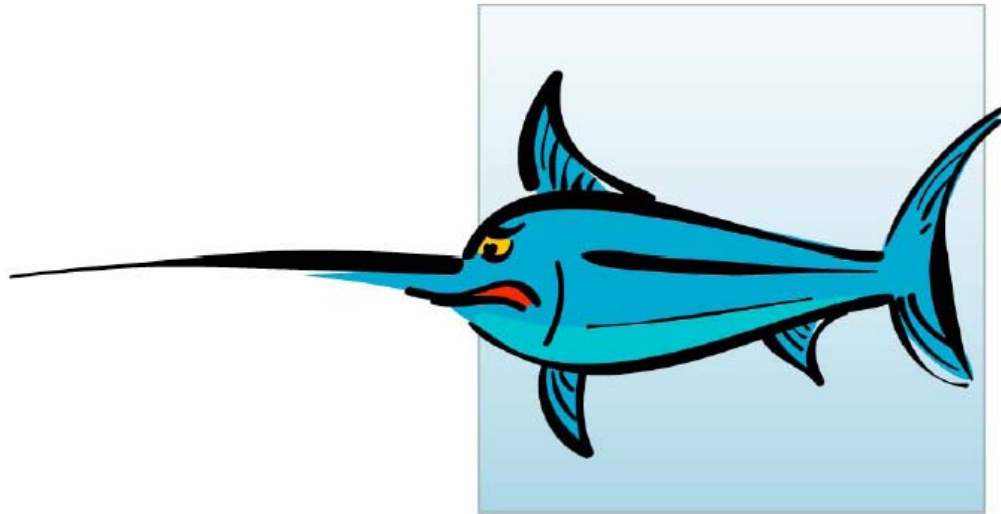


Post-ataque

- ❑ Desactivación de la infraestructura de ataque
- ❑ Borrado de rastros
- ❑ Evaluación del éxito del ataque
- ❑ Calibración de la respuesta de la entidad atacada y de las fuerzas del orden
- ❑ Aplicación de las lecciones aprendidas a la planificación del próximo ataque

Taxonomía de Phishing

- ❑ Atendiendo a
 - ❑ El canal de contacto
 - ❑ La falsa fachada
- ❑ Demo de algunos de ellos



Canal de contacto

- ❑ Inserción del hiperenlace en
 - ❑ Mensaje de correo
 - ❑ Mensaje instantáneo
 - ❑ IRC
 - ❑ Contenido web
 - ❑ Cualquier soporte de hiperenlaces: documento Word, PDF
- ❑ Modo de envío de los mensajes: ordenadores comprometidos con troyanos
 - ❑ Reclamo para instalar el troyano: SEX, SEX, SEX

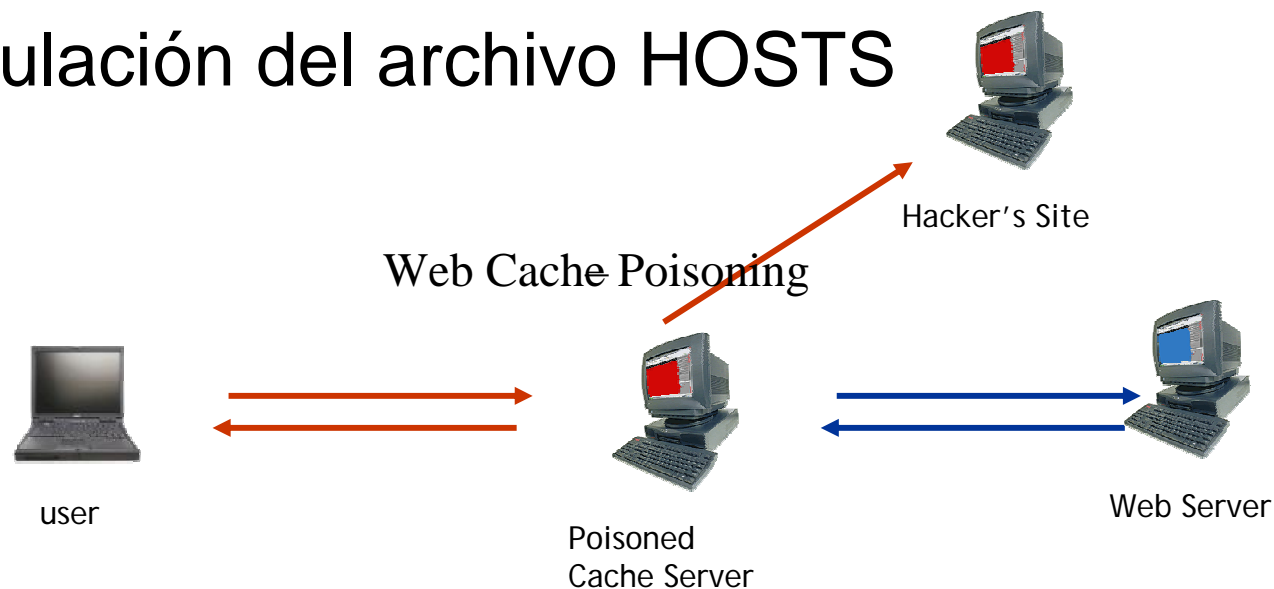


Falsa fachada

- ❑ Tipos de ataques
 - ❑ Hombre en el medio (MITM)
 - ❑ Ofuscación de URL
 - ❑ XSS
 - ❑ Fijación de sesión
 - ❑ Maquillaje
 - ❑ Espionaje del usuario

Hombre en el medio (MITM)

- ❑ Proxies transparentes
- ❑ Envenenamiento de caché DNS
- ❑ Ofuscación de URL
- ❑ Configuración del proxy del navegador
- ❑ Manipulación del archivo HOSTS



Ofuscación de URL

- ❑ Nombres de dominio similares
- ❑ Utilización del login para simular nombre de dominio: desactivado en las últimas versiones de los navegadores
 - ❑ `http://www.gruposantander.es:login.jsp?CodigoActivacionSeguridad=@3368601800`
- ❑ URL abreviados
 - ❑ `http://tinyurl.com/3erp1`

Cross-Site Scripting (XSS)

- ❑ El hiperenlace conduce al sitio verdadero
 - ❑ Todo es auténtico
 - ❑ Los certificados digitales también
 - ❑ Se inserta código para que el formulario se envíe al sitio web del phisher

Fijación de sesión

- ❑ El hiperenlace conduce al sitio verdadero
 - ❑ Todo es auténtico
 - ❑ Los certificados digitales también
 - ❑ Se crea una sesión para que al autenticarse la víctima utilice el mismo testigo
 - ❑ Conocido el testigo, se puede acceder a sus datos

Maquillaje

- ❑ Manipulación del aspecto del navegador que ve el usuario:
 - ❑ Marcos ocultos
 - ❑ Sobrescritura del contenido
 - ❑ Substitución gráfica

Espionaje del usuario

- ❑ Registro de la actividad del usuario
 - ❑ Keyloggers: hardware y software
 - ❑ Screenshot grabbers

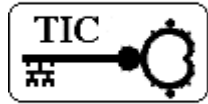


Soluciones contra el Phishing

- ❑ Raíz del problema: identidad digital débil
- ❑ Solución ideal: mecanismos de autenticación robustos
- ❑ Soluciones actuales: parches, marketing, medidas insuficientes



'En Internet nadie sabe que eres un perro'



¿Preguntas?

gonzaloalvarez.com

Creative Commons Attribution-ShareAlike 2.0

You are free:

- to copy, distribute, display, and perform this work
- to make commercial use of this work

Under the following conditions:



Attribution. You must give the original author credit.



Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the author.

Your fair use and other rights are in no way affected by the above.

This work is licensed under the Creative Commons Attribution-ShareAlike License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/2.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.