pue | 20 YEARS EMPOWERING TECHNOLOGY 1998-2018

Phishing

La evolución indetectable y cómo proteger a tu organización

Phishing

Qué es el Phishing.

Distintos tipos de Phishing.

Técnicas de creación básicas.

Ocultación de URLs.

Técnicas avanzadas.

Detección y protección.

Fernando Ruiz-Tapiador
Fernando@Ruiz-Tapiador.com
RHCA, C|EH, C|BP

Phishing

Qué es el Phishing.

Phishing

- El término viene de *fishing*, en el sentido de lanzar el anzuelo y ver que se pesca.
- Aparece por primera vez en 1996.
- El objetivo es robo de datos, de credenciales, tarjetas de crédito…

Phishing

- Principal mecanismo de transmisión de malware.
- Afecta a todas las plataformas.
- **Es el usuario el que instala el malware**.
- Difícil de detectar, imposible para usuarios no preparados.

Características del Phishing

- Suele tener un sentido de urgencia, que hagas alguna tarea antes de un tiempo determinado.
- Amenazan con cerrar la cuenta, cobrar algo, perder un gran descuento, paquete pagado…
- phishstats.info

Phishing

Distintos tipos de Phishing.

Tipos de Phishing

- SMiShing (SMS Phishing)
- Spimming (Spam over Instant Messaging)
- Vishing (Voice or VoIP Phishing)
- Spear Phishing (Dirigido a una persona concreta)
- Whaling (VIP Phishing)

Phishing

Técnicas de creación básicas.

URLs Simuladas

Missatge de text
avui 10:18

Abono por transferencia a su favor recibida en euros. Confirmar : http://bancosantander.es.online-es.mywire.org/recibo

Typosquatting

- Aprovechando errores tipográficos, registran dominios con el nombre parecido al legítimo:

www.gogle.es

www.goggle.com

@

- Todo lo que va delante de la @ en una URL, es el nombre de usuario de la web remota.
- Lo siguiente es ofuscar la web destino, poniendo la IP en otros formatos: decimal, hexadecimal…

www.realoviedo.es

www.realoviedo.es@B2F90884

www.realoviedo.es@3002665092

www.realoviedo.es@178.249.8.132

www.realoviedo.es@www.realsporting.com

Ataque XSS no persistente (indirecto)

- Añade un código a ejecutar en la parte del cliente

  www.paginaweb.es<script>alert(“Test”);</script>

- Tiene muchas variantes.

  es.wikipedia.org/wiki/Cross-site_scripting

Ataque XSS persistente (directo)

- Consiste en publicar el código a ejecutar, en el contenido de una página: foros, comentarios, posts…
- El contenido queda guardado en la página.
- Cualquiera que acceda a ella, lo ejecuta.

Phishing

Ocultación de URLs.

Acortadores

- Los acortadores ocultan la URL.
- Si pinchamos, vamos directamente sin ver la URL destino.

unshorten.link - “des-acortador” de URLs

QRs

- Con los QRs tampoco vemos las URLs.
- Chequear la URL antes de abrirla, o guardarla para más adelante.

Phishing

Técnicas avanzadas.

Ataques homográficos I

www.apple.com – Si es Apple

www.apple.com – No es Apple – la l del

l del dominio es una “i” mayúscula.

- Depende del tipo de letra, será más o menos obvio el “cambiazo”.

Ataques homográficos II

www.apple.com – Si es Apple

www.apple.com – No es Apple – la “a” es una

“a” cirílica, que es igual que la latina.

es.wikipedia.org/wiki/Nombre_de_dominio_internacionalizado

Ataques homográficos III

www.apple.com – Si es Apple

www.appmoc.el – No es Apple (probar a

a cortar y pegar la URL en otros sitios)

- El carácter Unicode *202e* (en la URL anterior, después de la segunda p) indica un cambio de sentido en la escritura.

Ataques homográficos III cont.

- Depende del programa, sistema operativo o navegador, los manejan de una forma u otra.
- Afortunadamente, los navegadores actuales no lo admiten en mitad de las URLs.

unicode-table.com/en/202E/

Phishing

Detección y protección.

Comprobadores de URLs

www.virustotal.com/gui/home/url

sitecheck.sucuri.net

scanner.pcrisk.com

www.urlvoid.com

Ataque homográfico

- **Firefox**: en **about:config** poner el parámetro:

  network.IDN_show_punycode a *true*

  punycode.es

  www.privacytools.io/browsers/#addons

Recursos generales recomendados

- www.privacytools.io - Gran recopilación, cambiando a Español hay un gran resumen:
  - victorhck.gitlab.io/privacytools-es/
- Otros plugins:
  - antivirus.comodo.com/online-security.php
  - www.bitdefender.com/solutions/trafficlight.html

¡Gracias!

Contáctanos.
Estamos para
ayudarte

Fernando Ruiz-Tapiador

fernando@ruiz-tapiador.com

Blog blog.pue.es

@ticPUE

pue IT CONSULTING & TRAINING

pue IT CONSULTING & TRAINING

SEDE BARCELONA

Av. Diagonal, 98-100
08019 Barcelona
T. 93 206 02 49

SEDE MADRID

c/ Arregui y Aruej, 25-27
28007 Madrid
T. 91 162 06 69