Si hace unos días hablábamos del misterioso Clickjacking como la madre de todas las vulnerabilidades en navegadores, hoy Giorgio Maone nos explica
cómo protegernos
frente a la amenaza... si es que podemos.

En resumen:

1. Los usuarios de **Firefox + NoScript** están a salvo del Clickjacking.
2. Los usuarios de **navegadores en modo texto** (Links , Lynx , w3m ...) están a salvo.
3. Los usuarios de **Opera** están a salvo del Clickjacking, siempre que sigan los siguientes pasos:

- Deshabilitar todas las opciones en Herrramientas -> Avanzado -> Contenidos.
- Escribir "opera:config" en la barra de direcciones. Buscar "Extensions" y deshabilitar "iFrames".

- Los usuarios de **Explorer, Safari y Chrome** no disponen de ninguna protección totalmente eficaz frente al Clickjacking.

Y algunas observaciones interesantes en los comentarios en el artículo de kriptópolis :

Noscript para Firefox no es suficiente

Parece que la proteccion que brinda Noscript para Firefox no es suficiente, pueden ver aqui un post sobre como bypassear la seguridad solo con simples ideas:

http://nulledcore.com/?p=117

Con la etiqueta de object se puede hacer un iframe el cual Noscript no detecta como malicioso por lo cual puede que aun estando con el addon en Firefox sigamos estando en riesgo.

Por Julian A. Rodriguez

¿Vale la pena seguir navegando bajo esas condiciones?

Si estamos en modo paranoico pues NO. Solamente usando vulnerabilidades conocidas resulta que estamos absolutamente desprotegidos y que además no podemos hacer nada al respecto:

- No podemos fiarnos de las resoluciones de nuestros DNS ya que podrían estar envenenadas, con lo cual la página podría no ser la que creemos estar visitando.

- El contenido de la página puede lanzar acciones como si las hubiera seleccionado el usuario. Por lo visto en este hilo, ninguna protección antiscripts puede evitar eso.

- Dichas acciones pueden acabar permitiendo la ejecución de código arbitrario en nuestro equipo, incluyendo la descarga de nuevo código.

- Dicho código puede instalarse como rootkit y/o meter a nuestro equipo en una botnet ante la mirada impasible de nuestro antivirus.

¿Me lo parece a mi o estamos perdidos?

Una posible solución

Si utilizas algún tipo de *ix hay algo que puedes hacer para mitigar el impacto.

El primer requisito es el de siempre: navegar usando una cuenta de usuario normal, nunca como root.

El segundo, tener el /home en una partición aparte.

Por último, dicha partición debe ser montada SIN el flag que permite la ejecución de "aplicaciones/programas/scripts/etc.".

De esta manera no es posible ejecutar absolutamente nada que resida en dicha partición, y si tienes el cuidado de sólo utilizar un usuario "normal" para navegar Internet, entonces cualquier cosa que te bajes va a copiarse sobre dicha partición desde la que no puede ejecutarse.

La desventaja de esto es que no puedes utilizar /home para instalar aplicaciones/scrips. Pero para ello existe /usr/local.

Ah me olvidaba, /tmp también debería ser "capado" (te puedes hacer un bonito symlink a algún directorio en /home).

Nota: No sé qué efecto esto tenga para controlar scripts de perl/python o "binarios" java (por ejemplo applets que vengan desde la red). Tendria que probarlo.

...

La supuesta vulnerabilidad no "copia" un ejecutable a tu disco, sino que lo ejecuta el navegador directamente.

De hecho, un peligro potencial es que gracias a la vulnerabilidad se ejecute un código que *envíe*

ficheros de tus discos al servidor web remoto. Tampoco ayuda en nada montar discos con noexec en este caso.

Con respecto a lo de usar una cuenta de usuario normal, no administrativa, estoy 100% de acuerdo. Este consejo también sirve para Windows, y tiene exactamente el mismo efecto que en Linux.

Por último, recomendaría utilizar VMWare, instalar una máquina virtual nueva con tu distribución y navegador preferidos, configurar los discos como " Nonpersistent " ***ANTES*** de comenzar a navegar y luego utilizar siempre esta máquina virtual en vez de un navegador de verdad en tu máquina real.