C /Cabana 5-7 Bajo
15006 A Coruña
T 981 912 305
F 981 065 200
E irix@irix.es

D. Miguel Mosquera Montero, Licenciado en Informática, miembro del cuerpo oficial de peritos del CPEIG (Nº colegiado: 00077), actuando a solicitud de D. Juan Carlos González Santín con DNI 33313488N, y domicilio en Rúa Esquecemento 4 2º, Lugo, emite el siguiente:

INFORME

1.- OBJETIVOS

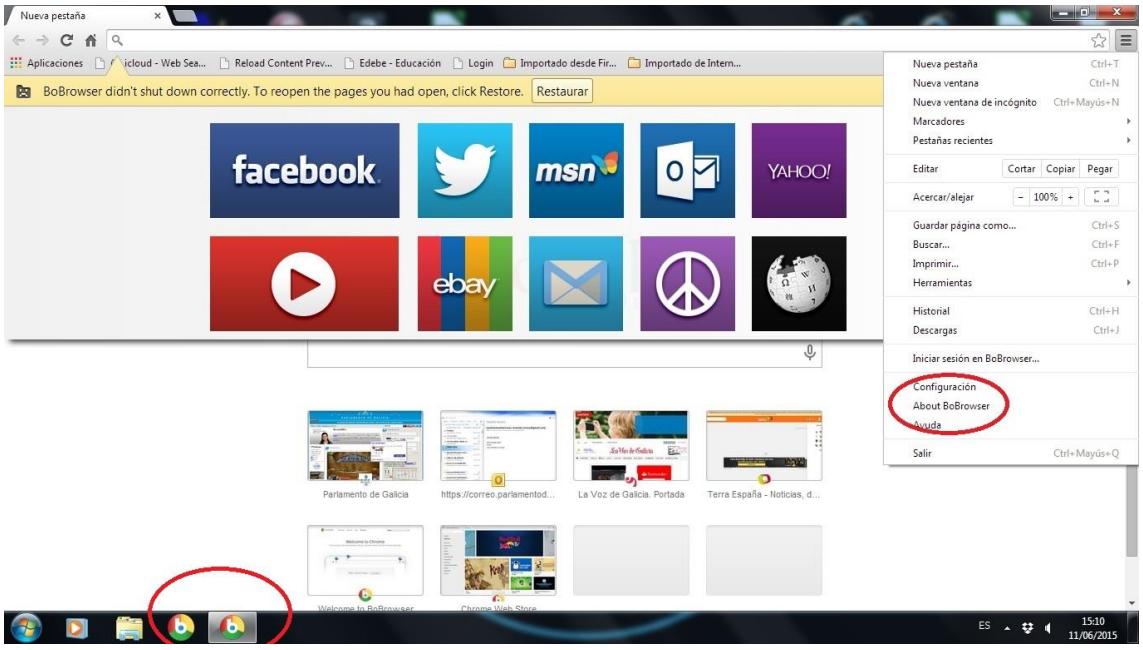
El objetivo del presente informe es determinar la veracidad de los hechos publicados en diversos medios de comunicación (abc, el economista, twitter,...) donde se afirma que D. Juan Carlos consultaba una web erótica en el trascurso de una sesión parlamentaria el pasado martes día 9 de Junio de 2015.

2.- ESTUDIO REALIZADO

El día 11 de Junio de 2015, sobre las 15:00 horas, D. Julio Ballesteros como abogado de D. Juan Carlos, nos hace entrega en nuestras oficinas de A Coruña un ordenador portátil de marca Toshiba.

Procedemos a examinar el equipo informático que nos muestran. El ordenador analizado se trata de un equipo portátil Toshiba Portege Z930-149, con Part. Number: PT234E-06D04JCE y Serial Number: YC015739H, con nombre de equipo PORTATILIX37 y sistema operativo Windows 7 Professional.

Al arrancar dicho ordenador comprobamos que automáticamente se inicia un navegador de internet.



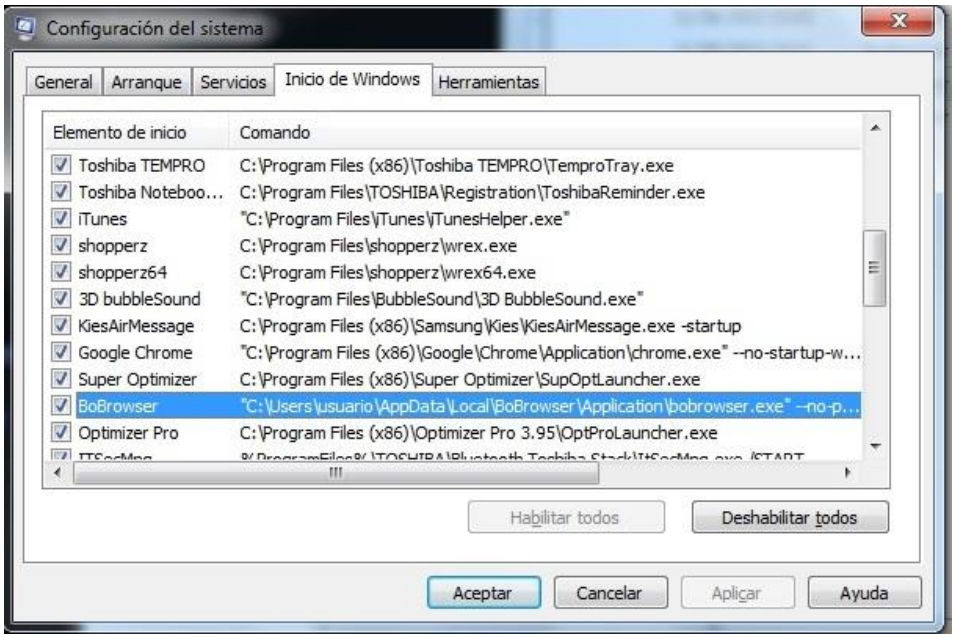
Como se puede ver en la imagen anterior, dicho navegador, tiene un icono muy similar al del conocido Google Chrome.

 Bobrowser  Google Chrome

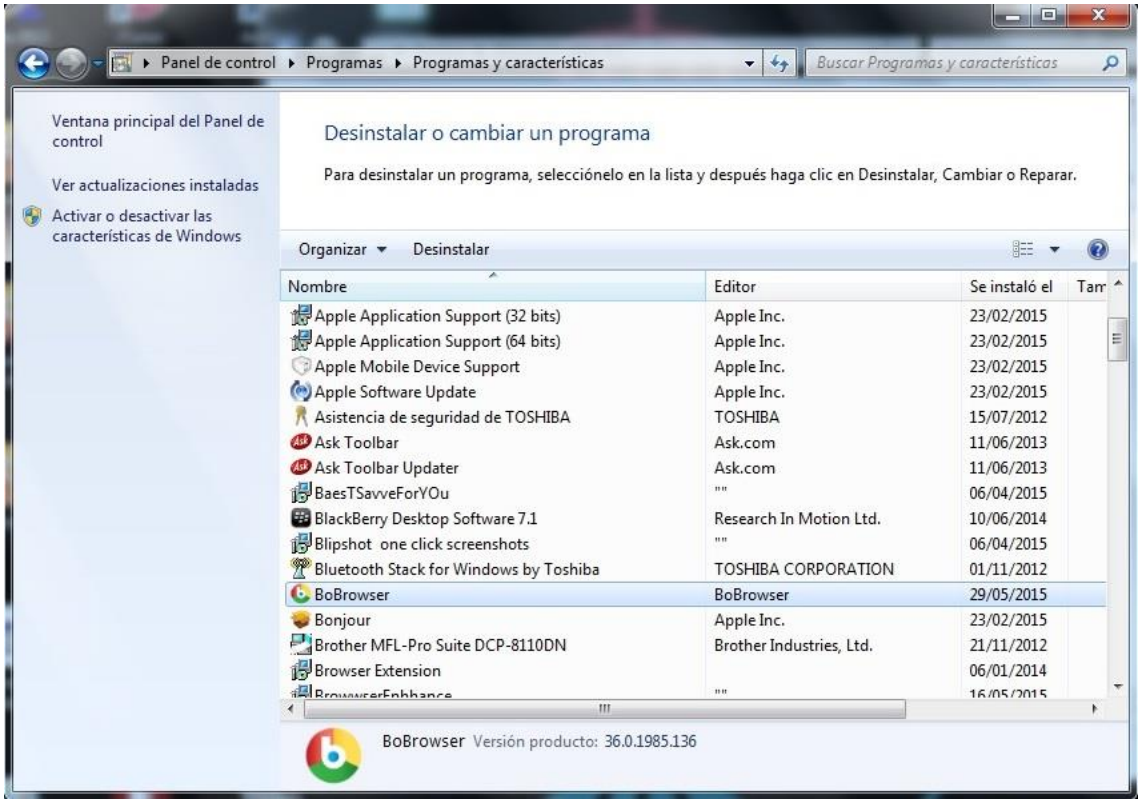
Sin embargo se trata de un software considerado como programa potencialmente no deseado denominado BoBrowser. Dicho software es capaz de infiltrase en los ordenadores sin que el usuario sea consciente de ello, por ejemplo siendo incluido como paquete en utilidades gratuitas, y su misión principal es alterar las preferencias de navegación de internet del usuario, así como inundar los navegadores web con ventanas emergentes, pop-ups, banners,…. de contenido publicitario falso, y que aparecen automáticamente.

Lo primero que observamos es que sin interactuar con el equipo, al poco tiempo se abren automáticamente ventanas de publicidad.

Gracias a la utilidad msconfig, se comprueba que el software malicioso está configurado en el inicio de Windows, motivo por el cual, nada más arrancar el ordenador ya nos aparece automáticamente.

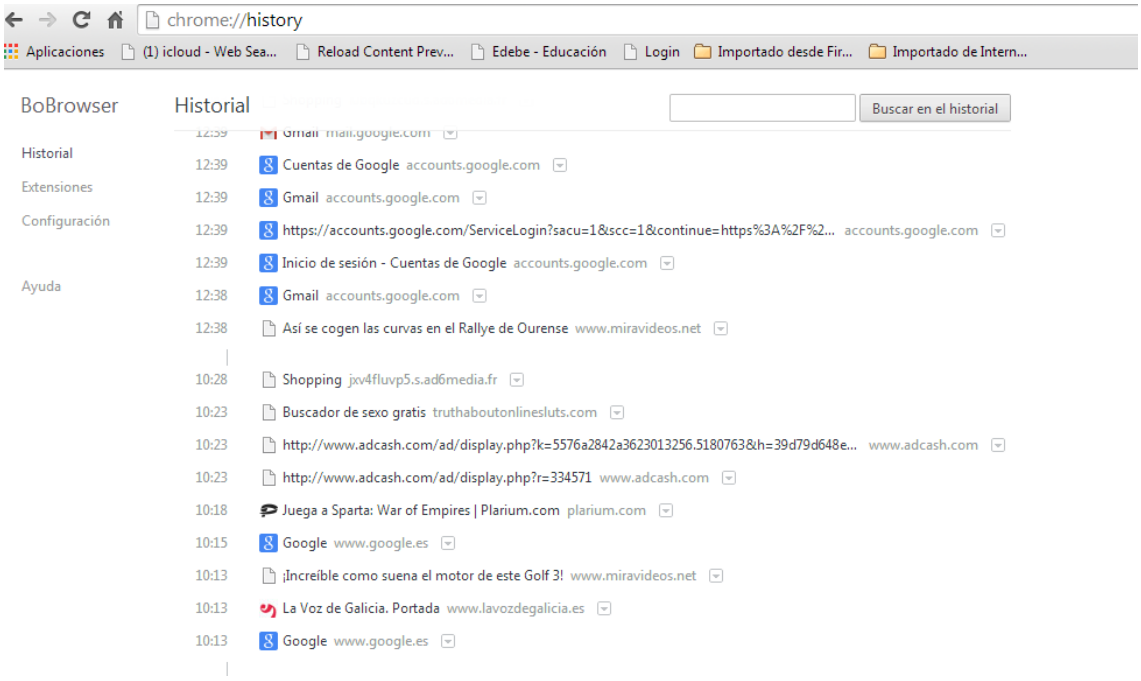


Lo siguiente que nos interesa comprobar es desde cuando está instalado este software. En el panel de control de Windows, Programas, Programas y características, obtenemos esa información. El programa ha sido instalado el día 29 de Mayo de 2015.



Intentamos navegar por internet con el navegador infectado y se abren páginas automáticamente, el navegador funciona muy lento y no responde correctamente a las acciones habituales, tales como desplazarse por las webs y continuamente se encuentra redireccionando enlaces, no termina de cargar la página deseada.

En función de la noticia publicada, accedemos al historial del navegador, y nos centramos en el pasado día martes 9 de Junio. A continuación podemos observar en la imagen lo que nos aparece en el historial:



Según nos comenta D. Juan Carlos, ese día comenzó la sesión parlamentaria a partir de las 10 de la mañana. Vemos que el primer link guardado es el del buscador google, www.google.es, y a continuación la web del periódico la voz de Galicia. Automáticamente, un link publicitario de la web miravideos.net, que además es uno de los links que nos ha saltado automáticamente durante el presente estudio. Todo esto en el mismo minuto, a las 10:13. Dos minutos más tarde se vuelve al buscador google y a continuación una nueva página publicitaria del juego Sparta: War of Empires y los siguientes links, son claves en este estudio. A las 10:23, en el mismo minuto se abren 3 links, primero 2 del dominio adcash.com y a continuación otra de buscador de sexo gratis truthaboutonlinesluts.com. Adcash es otro programa adware con el mismo fin publicitario de Bobrowser y que bombardea continuamente con pop-ups y banners publicitarios que aparecen automáticamente.

Comprobamos que el tercero de los enlaces corresponde al siguiente link:

http://truthaboutonlinesluts.com/es/xxx/?voluumdata=vid..00000003-6932-43b7-8000-000000000000__vpid..c4774800-1039-11e5-82a8-6a4c7c8b78e3__caid..1a6a8f55-8e42-4417-9cf8-481562353cb9__rt..R__lid..0eb237dc-62ed-4c74-8bed-3dfb2b5406f6__oid1..e2701c37-3a6d-407b-96f9-57c1622cfdf6__var1..334571__var2..15343479471434030705__rd..www%5C.%5Cadcash%5C.%5Ccom&source=334571&acclickid=15343479471434030705

y que lleva automáticamente a la siguiente imagen, sin tener que realizar ningún click ni teclear nada:

Que es la imagen que aparece publicada en los medios de comunicación y asociada a una web erótica. Como se podrá observar por la complejidad del link, es virtualmente imposible que se haya tecleado manualmente y sin equivocación ese link y los dos anteriores en el espacio de un minuto.

Por último, hay que reseñar, tal y como se puede ver en los links posteriores en el historial (shopping, rallye, Gmail,…), que no se ha clicado en el sitio web ofertado ni en ninguna página de contenido erótico.

3.- CONCLUSIONES

En base al análisis efectuado, se concluye lo siguiente:

1. Al iniciar el equipo portátil analizado se arranca automáticamente el software malicioso BoBrowser.

2. BoBrowser está catalogado como PUP (programa potencialmente no deseado) y se instala como complemento de los navegadores de internet y de similar apariencia.

3. Dicho software es capaz de infiltrase en los ordenadores sin que el usuario sea consciente de ello, por ejemplo siendo incluido como paquete en utilidades gratuitas.

4. La misión principal de este software es alterar las preferencias de navegación de internet del usuario, así como inundar los navegadores web con ventanas emergentes, banners, pop-ups,…. de contenido publicitario falso, y que aparecen automáticamente.

5. BoBrowser fue instalado en el equipo el 29/05/2015 con anterioridad a la noticia publicada.

6. BoBrowser se inicia automáticamente con inicio Windows sin necesidad de actuación por parte del usuario.

7. Durante la realización del estudio, se observa que automáticamente se generan distintas ventanas de publicidad entre otras referidas a adcash.com, calificado también de software malicioso.

8. En el historial de navegación del martes, se puede ver que existe un link de adcash a las 10:23 que abre automáticamente otro popup con la foto aparecida en los medios de comunicación.

9. Si se analiza la complejidad y longitud del link que referencia esa foto, no parece que sea posible teclearlo sin fallos y en menos de un minuto.

10. Durante el examen esa misma página ha aparecido automáticamente.

Queda demostrado pues, que el equipo portátil de D. Juan Carlos lleva infectado por software malicioso desde el 29 de Mayo, y dicha infección ha provocado la apertura automática de la página publicada en los medios, sin acción voluntaria por parte del usuario.

Lo que hago constar, según mi leal saber y entender, en A Coruña a once de Junio de dos mil quince.

Fdo.: Miguel Mosquera Montero