**Drive By Download.**

El ataque de Drive By Download es una técnica que ha sido utilizada por ciberdelincuentes. Se basa en el hecho de visitar una página web que esté infectada y ya con el simple hecho de acceder a ella, el malware de manera oculta se ha instalado en nuestro equipo; podemos observar que no es necesario que se descargue ningún archivo ni nada, simplemente el malware se encuentra dentro del código (HTML) de la página web por lo que solo el hecho de abrirla hace que nuestro equipo esté infectado.

Este tipo de malwares se aprovecha de los equipos desactualizados y con fallas de seguridad para explotar sus vulnerabilidades y de esta forma poder instalar el software malicioso de manera automática. Dentro de las páginas afectadas no solo se encuentran las páginas de alto riesgo, en los últimos años los hackers han modificado páginas legítimas y confiables para que contengan dentro de su código este tipo de malwares.

Por lo general las partes que son modificadas suelen ser: el código JavaScript, Adobe Flash, iFrames, links, etc. El código que generan este tipo de malwares no es complejo, debido a que su objetivo es contactar con otra computadora desde donde se introducirá el resto del código necesario para que se pueda acceder tanto al móvil como al ordenador.

Las fuentes de infección no solo se limitan a las visitas de páginas web, también pueden ocurrir mediante un mensaje de correo electrónico o accediendo a alguna ventana emergente (puede que estas estén diseñadas usando técnicas de ingeniería social.)

Referencias:

<https://www.cert.gov.py/index.php/noticias/ataque-drive-download-ataques-desde-webs-legitimas>

<https://www.mcafee.com/blogs/consumer/drive-by-download/>

<https://www.aboutespanol.com/que-es-drive-by-download-157893>