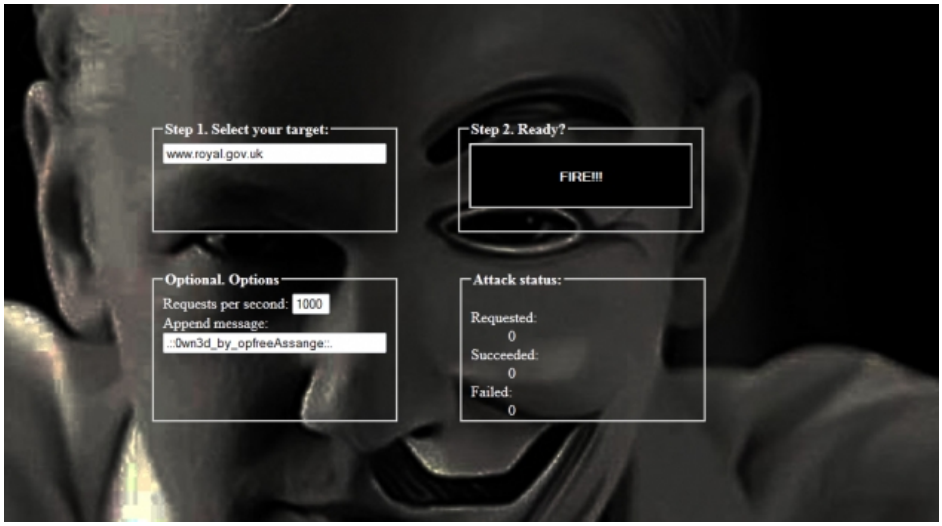

A Fundación de Fronteras Electrónicas publica unha serie de consellos para axudar a webs pequenas e independentes a evitar os ataques distribuídos de denegación de servizo ou DDoS.

A Fundación de Fronteiras Electrónicas (EFF, nas súas siglas en inglés) distribuíu unha guía e un vídeo para axudar aos xestores de páxinas web de todo o mundo a evitar un dos ataques máis simples e destrutivos de internet: o ataque distribuído de denegación de servizo ou DDoS. O organismo, dedicado a vixiar a liberdade de expresión e loitar contra a censura na rede, cre que, aínda que ás grandes organizacións non lles custa demasiado recuperarse destes ataques, cada vez máis comúns, “os sitios máis pequenos, como os que pertencen a medios independentes ou organizacións de dereitos humanos, poden verse afectados de forma permanente”, di Jillian York, directora do departamento de Liberdade de Expresión Internacional de EFF, nunha nota.

Baixo a lema “non deixes que che silencien”, a guía aconsella tomar dúas medidas moi concretas que se resumen en dúas palabras en ínguas: mirror (espello) e backup (copia de seguridade). Os espellos son copias da web que conteñen a mesma información que teñen estas, aínda que son copias estáticas, é dicir, que non se poden realizar accións como editar os contidos. A maior parte das empresas de aloxamento web ofrecen este servizo, e tamén o fan páxinas gratuíta como Blogger ou WordPress .

{youtube}I6HgLcMmIKk{/youtube}

As copias de seguridade , pola súa banda, son fundamentais para non perder todo o contido dunha web en caso de ataque. Segundo explica a guía, en un servizo de aloxamento é necesario exportar todas as páxinas, entradas e comentarios a un único arquivo XML, aínda que só se gardarán os textos, e non outros contidos, como imaxes. Se o usuario executa o seu propio servidor web, debe configurar as copias de seguridade automáticas a un servidor remoto; algunhas ferramentas útiles para facelo son ssh , scp , mysqldump e crontab . A web explica como realizar esas copias, paso a paso.

“A falta de recursos ou de coñecemento pode significar que unhas webs son máis vulnerables que outras”, di Eva Galperin, coordinadora do departamento de Liberdade de Expresión Internacional de EFF. ”Queremos ofrecer a eses sitios as ferramentas que necesitan para protexer os seus contidos”, engade. A guía tamén ofrece un cadro cos servizos de aloxamento máis populares, e os seus prezos, aínda que algúns se reducen ao mercado anglosaxón.

Ademais deses pasos aconsellados na guía da EFF, os expertos recomendan tamén non aloxar a web e o DNS (a dirección da páxina) no mesmo sitio, xa que, en caso de ataque a unha dirección IP específica, esta prevención permite reacoller a web.

DDoS: unha ferramenta de ataque ou de defensa? O ataque distribuído de denegación de servizo (ou DDoS, nas súas siglas en iglés) é un dos máis habituais en internet, xa que é simple e efectivo: o atacante sincroniza un grupo de sistemas para que visiten de forma coordinada e no mesmo momento unha determinada web e así consegue tombala, xa que as múltiples peticións realizadas saturan o ancho de banda da que esta dispón.

O DDoS foi utilizado tanto por axencias gobernamentais para silenciar webs incómodas (como no caso recente de Wikileaks) como por activistas que o usan para, á súa vez, atacar obxectivos gobernamentais. O DDoS é, de feito, a ferramenta favorita de Anonymous. Hai só uns días, o grupo de ciberactivistas lanzou un ataque deste tipo contra diferentes páxinas do Goberno británico en protesta polo acoso a Julian Assange, o fundador de Wikileaks, refuxiado na embaixada de Ecuador en Londres.

EFF, que loita polas liberdades civís en internet, é consciente de que o DDoS pode ser utilizado, en ocasións, para defender esas liberdades. Por iso, os seus responsables non queren pronunciarse sobre a ferramenta en si. “O problema cos ataques DDoS”, reflexiona Jillian York, directora do departamento de Liberdade de Expresión Internacional de EFF, “é

que, aínda que foron usados polos cidadáns en accións directas, por exemplo contra Mastercard e Visa [polo caso Wikileaks], tamén son utilizados con demasiada frecuencia contra páxinas pequenas e independentes, como as de blogueros, xornalistas cidadáns ou organizacións de dereitos humanos". Por iso, conclúe York, "é imposible que teñamos unha única visión sobre o DDoS". En todo caso, a guía, insiste a activista, "non está pensada para Visa ou outras grandes empresas, se non para eses sitios pequenos ou independentes".