Nacióddigital
DES DE 1996

Tecnologia | Redacció | Actualitzat el 22/10/2016 a les 18:00

Els atacs informàtics a l'era de la Internet de les coses

La caiguda de serveis com Twitter o Spotify ha estat possible gràcies a la planificació dels atacants | La manca de seguretat dels aparells i dispositius que es connecten a Internet facilita els ciberatacs

Estat dels atacs DDoS | Digital Attack Map

Aquest divendres, diversos webs com Twitter, Amazon, Netflix, CNN, Reddit, Ney York Times, SoundCloud, AirBnB, Github, PayPal o Spotify, entre d'altres, han resultat víctimes d'un atac informàtic (http://www.naciodigital.cat/noticia/118271/atac/informatic/afecta/twitter/spotify/mitjans/new/york/times) que ha provocat que no fossin accessibles durant algunes hores.

L'atac, però, no s'havia centrat en cap d'aquests webs en particular sinó en un proveïdor que totes tenen en comú, **Dyn**, una companyia que ofereix serveis de resolució de noms de domini (DNS). Així, la principal diferència d'aquest atac amb altres que tenien com a objectiu un web concret és que en aquest cas s'ha optat per centrar-se en un dels possibles punts febles que compartien moltes empreses que utilitzaven els serveis de Dyn, tot realitzant un **DDoS** contra la infraestructura de la companyia.

DDoS, un atac distribuït i difícil d'evitar

Els atacs de denegació de servei distribuïts (les sigles en anglès de les quals són DDoS, de *Distributed Denial of Service*) són molt simples: es tracta de fer que molts dispositius enviïn, al mateix temps, moltes dades a un servidor d'Internet determinat. D'aquesta manera, el servidor que n'és víctima no és capaç de respondre a totes les sol·licituds que rep i deixa de funcionar amb normalitat.

Com que les peticions arriben des de moltes màquines diferents, la tasca de defensar-se'n es complica ja que no és tant fàcil detectar quines sol·licituds són d'usuaris que intenten visitar webs i quines són part de l'atac en si mateix. A més, tal com ha informat Dyn, en total va rebre tres atacs diferents (https://www.dynstatus.com/) durant el dia.

El servei de DNS, un dels objectius dèbils

El DNS o sistema de noms de domini (https://ca.wikipedia.org/wiki/Domain_Name_System) és una base de dades distribuïda que s'encarrega de *resoldre* els noms de domini (com naciodigital.cat, google.com o qualsevol altre domini d'Internet) per tal de trobar l'adreça IP (https://ca.wikipedia.org/wiki/Adre%C3%A7a_IP) del servidor que té la informació del web o correus electrònics, entre d'altres. Seria, en resum, com una guia telefònica de dominis.

Degut al gran número de dominis que hi ha avui en dia, el DNS és un dels elements tècnics més complexos d'entendre i gestionar. Un dels exemples és que un canvi de configuració pot tardar diverses hores -o fins i tot dies- en fer-se efectiu en alguns casos, de manera que quan un servidor DNS deixa de funcionar, els canvis necessaris podrien tardar tant en replicar-se que l'atac ja s'hauria acabat.

A més, en aquest cas ens trobem amb una sola empresa que gestionava els DNS de molts webs amb un trànsit important, fet pel qual, a més dels atacs per si mateixos, que van implicar molt trànsit addicional, també ha estat més visible que si s'hagués escollit alguna altra empresa com a objectiu.

La Internet de les coses i els atacs distribuïts

Un altre dels elements a tenir en compte és el de la Internet de les coses: cada cop hi ha més dispositius diferents connectats a la xarxa. Ja no només podem comptar ordinadors de sobretaula o portàtils, sinó que, més enllà dels mòbils, hi ha càmeres sense fils, termostats, cotxes... I hem de tenir en compte que qualsevol dispositiu és susceptible de ser controlat de forma remota si un atacant pot aprofitar alguna vulnerabilitat de seguretat per a instal·lar-li un programa per controlar-lo.

De fet, tampoc hauríem d'oblidar que en alguns casos, els dispositius s'acaben controlant gràcies a haver aconseguit les dades d'accés preguntant-les directament -per correu electrònic, per exemple- a l'usuari que l'utilitza, tot fent-se passar per banc, informàtics o altres persones que serien de confiança. En altres casos, s'obté aconseguint que els usuaris s'instal·lin aplicacions mòbils amb *malware* -tot i que cada cop es controla més la seguretat de les apps a les botigues de les diferents plataformes.

I també hem de tenir en compte que aquesta mateixa setmana sortia a la llum una nova vulnerabilitat, que s'ha anomenat *Dirty Cow* (http://dirtycow.ninja/) , i que fa més de 9 anys que existeix però fins ara no s'ha fet pública ni s'ha corregit, i que feia que un atacant pogués actual com a administrador sense permís en sistemes Linux, que es troba en gran part dels servidors i en molts dispositius connectats -com els mòbils o aparells amb versions d'Android, per exemple.

Qui pot haver-hi darrere d'aquests atacs?

La resposta és complicada, perquè el fet que l'atac sigui distribuït fa que inicialment la informació que es pugui extreure sigui només la d'aparells que han estat *craquejats* per algun problema de seguretat, i una de les poques opcions de trobar-ne l'orígen seria accedir a algun d'aquests aparells esperant trobar la forma d'infecció que ha permès que s'utilitzin com a node d'atac i que aquesta contingui algun tipus d'informació rellevant sobre l'autor o autors.

En general, però, en atacs d'aquest tipus hi podríem trobar tres tipus d'interessos. Per un costat, sempre hi ha l'econòmic, a mode de segrest, on l'atacant pot demanar un rescat a canvi d'aturar

els atacs. En aquest cas, però, semblaria poc probable degut al ressò que ha tingut l'atac. Per altra banda, també hi ha el fet que alguns col·lectius que promouen aquest tipus d'atacs són precisament grups que solen ser contraris a que empreses com Twitter, precisament, emmagatzemin dades personals o tinguin massa control sobre la vida de les persones. En aquest cas, a falta de poder atacar objectius més grans com Facebook, l'opció de fer-ho amb altres webs importants, però més petits i amb un proveïdor en comú seria també viable. Finalment, també s'especulava amb l'opció d'una protesta per l'aïllament d'Internet de Julian Assange, després que Wikileaks hagi fet un tuit demanant que s'aturéssin els atacs.

Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point. pic.twitter.com/XVch196xyL (https://t.co/XVch196xyL)

? WikiLeaks (@wikileaks) 21 d'octubre de 2016
(https://twitter.com/wikileaks/status/789574436219449345)

Ens cal més seguretat informàtica a tots

Fixem-nos, doncs, que aquests atacs -com tants d'altres darrerament- s'han basat gairebé sempre en aturar serveis amb molts usuaris gràcies a atacs distribuïts. Uns atacs que són possibles només perquè en general no donem a la seguretat informàtica la importància que es mereix.

Sense saber-ho, un termòstat electrònic d'un veí podria haver estat part de l'atac. O el nostre telèfon mòbil, mentre caminàvem. O algun vehicle Tesla -o qualsevol amb Android Auto-, o algun rellotge intel·ligent. Potser una bombeta d'aquelles que permeten control d'intensitat de llum amb una aplicació mòbil. O directament l'enrutador d'Internet que tenim a casa. Qualsevol dispositiu podria ser insegur. I així com un ordinador té una pantalla des d'on insistir-nos -li fem cas o no, que seria molt recomanable fer-n'hi- que actualitzem perquè hi ha problemes de seguretat importants.

Però en sistemes *encastats*, en neveres, cotxes o robots aspiradors amb connexió a la xarxa, aquestes vulnerabilitats podrien ser-hi sempre, amagades, esperant que algú les utilitzés. I tant es podrien fer servir per atacar serveis d'Internet com per fer funcionar d'una manera determinada a distància, de manera que hem de ser conscients que, malgrat no suposar un perill massa greu, si que estem sobreexposats a fets que creiem que només passen a les pel·lícules. I en canvi, són totalment palpables ara mateix.