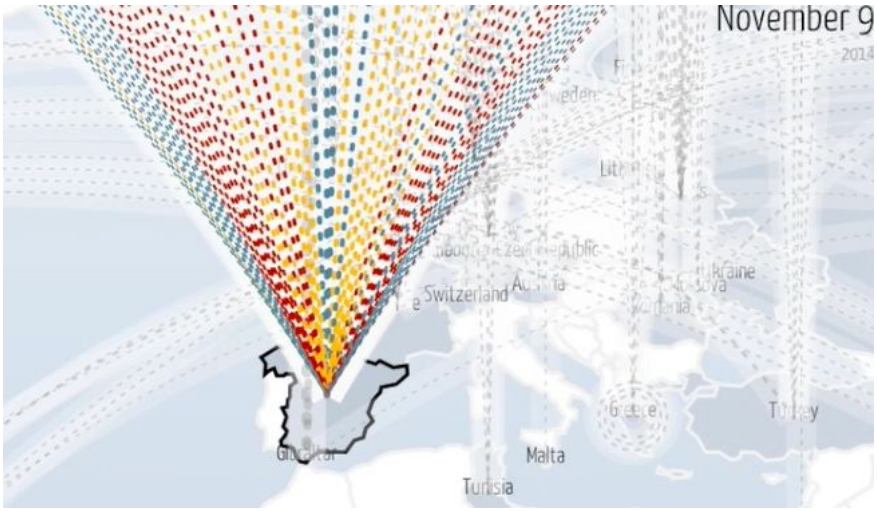
La ciberguerra del 9-N: així va ser l'atac informàtic al Govern

La Generalitat està convençuda que es van contractar especialistes per intentar impedir el procés participatiu

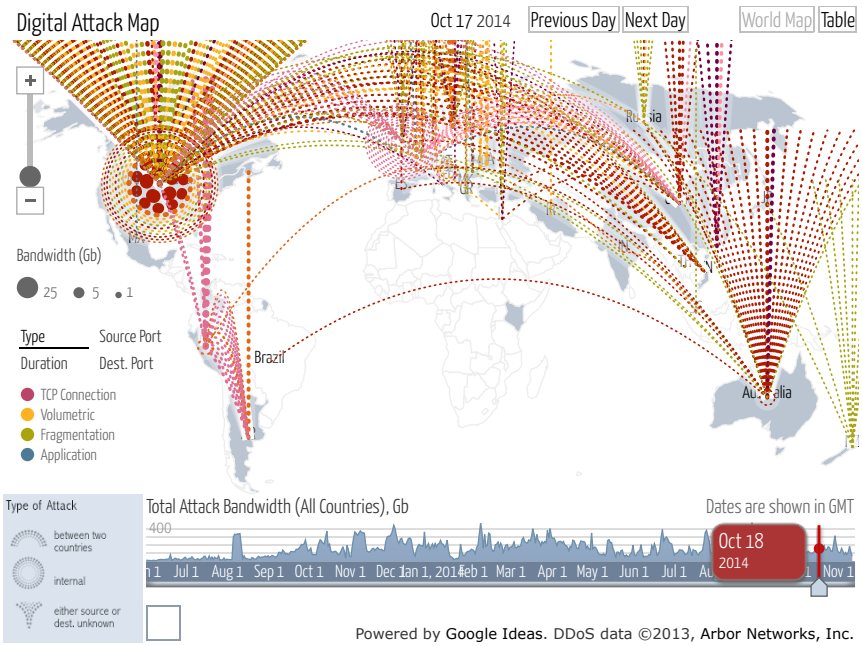
ENRIC BORRÀS Barcelona | Actualitzada el 11/11/2014 20:08



El cap de setmana passat la Generalitat "va rebre el ciberatac més important de la seva història", segons fonts del Govern. Un atac "molt dur" - ha reconegut aquest dimarts Artur Mas (http://www.ara.cat/politica/Mas-informatics-durissims-historials-electroniques_0_1246675517.html)- que va deixar fora de servei la web i el correu electrònic de la Generalitat, la web del president, el Servei Meteorològic de Catalunya, la recepta electrònica i l'accés dels professionals del Servei d'Emergències Mèdiques als historials clínics dels pacients. L'assalt també va disparar contra la pàgina oficial del 9-N, Participa2014.cat, però no va arribar a caure.

El Govern està convençut que va ser un ciberatac polític i que qui el va organitzar va contractar especialistes per fer-lo. L'objectiu era intentar impedir o posar traves al procés participatiu del 9-N, perjudicar la imatge de la Generalitat i fer més difícil que es pogués comunicar amb els ciutadans. El mateix dia també van rebre agressions (http://www.ara.cat/politica/ANC-Omnium-Ara_es_l-hora-9-N-boicot_0_1244875787.html) pàgines d'entitats com l'Assemblea Nacional Catalana (ANC). I membres de l'ANC, Òmnium Cultural i l'Associació de Municipis per la Independència van rebre desenes de milers de trucades sense interlocutor que, a la pràctica, els van bloquejar els telèfons.

Segons el Govern aquest cap de setmana només hi va haver tres ciberatacs més intensos a la resta del món i el 90% del trànsit a internet causat per atacs informàtics a l'Estat es va concentrar contra els servidors de la Generalitat. El Govern fa servir sistemes interns per treure aquestes conclusions però al vídeo de la notícia podeu comprovar fins a quin punt es van disparar els atacs informàtics a l'estat espanyol el cap de setmana passat. Hi podeu veure una representació dels ciberatacs a Europa entre l'1 i l'11 de novembre segons el Digital Attack Map (http://www.digitalattackmap.com/#anim=1&color=0&country=ES&time=16383&view=map), fet per l'empresa de seguretat Arbour Networks en col·laboració amb Google (http://www.digitalattackmap.com/about/). També podeu veure l'evolució dels atacs informàtics en aquest mapa interactiu (http://www.digitalattackmap.com/#anim=1&color=0&country=ES&time=16383&view=map):



L'escomesa als servidors de la Generalitat va començar a les onze del matí. El trànsit a les webs de la Generalitat va multiplicar per 20.000 el d'un dia normal. A les dotze del migdia ja hi havia pàgines i serveis que havien deixat de funcionar i es va detectar l'atac. El Centre de Seguretat de la Informació de Catalunya (Cesicat (https://www.cesicat.cat/)) va resoldre la situació entre les sis i les set de la tarda de dissabte i va blindar el sistema. Diumenge, el dia del 9-N, el trànsit a les webs del Govern va ser 60.000 vegades superior al d'un dia normal, però ja no va caure la xarxa. El dia 10 l'atac encara va continuar tot i que va ser molt menys intens.

Mercenaris d'internet

Tenint en compte que el 9-N era per preguntar sobre si Catalunya s'ha d'independitzar d'Espanya seria lògic pensar que l'atac el van organitzar unionistes. Josep Domingo-Ferrer (http://crises-deim.urv.cat/jdomingo/), director de la càtedra Unesco de Privadesa de Dades de la Universitat Rovira i Virgili, recorda que països com la Xina, la Índia i el Pakistan tenen unitats militars dedicades a la ciberguerra i que "qualsevol servei d'intel·ligència de qualsevol estat modern té 'hackers', encara que els contracta o forma de manera discreta". El govern espanyol, evidentment, té en nòmina experts en seguretat informàtica, però això no vol dir que hagi organitzat l'atac. I en aquest cas sembla que no ho va fer, com a mínim directament.

L'atac venia sobretot d'ordinadors dels Estats Units, però també d'Ucraïna, Rússia i la Xina, segons les dades del Cesicat. Això, i la mena d'agressió de què es tracta, duu Domingo-Ferrer i l'expert en seguretat informàtica José Nicolás Castellano (https://twitter.com/jncastellano) a pensar que el ciberatac es va fer contractant un especialista o una organització dedicada a aquesta mena de delictes. La Generalitat també creu que es va contractar un o més cibermercenaris per dur-lo a terme.

Castellano, president de No cON Name (https://www.noconname.org/), l'associació que organitza el congrés de 'hackers' més veterà de l'estat espanyol, explica que "per cinquanta o seixanta euros es pot contractar a través d'internet un atac d'aquesta mena contra una empresa normal"; com que el Govern està més preparat que una víctima convencional el preu podria ser una mica més alt, però tampoc gaire. Segons un estudi de TrendMicro (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf) sobre la ciberdelinqüència russa un ciberatac com el que va patir la Generalitat que duri una setmana sencera es pot comprar a partir de 150 dòlars. La Generalitat, amb tot, creu que va caldre "un pressupost considerable per fer-lo".

La mena d'agressió que van rebre les webs del Govern s'anomena atac distribuït de denegació de servei (DDoS). Quan un internauta visita una web el seu ordinador fa una petició d'informació al servidor que l'allotja, el navegador interpreta aquesta informació i mostra la pàgina a qui hi navega. Si molts ordinadors, alhora, demanen informació sense parar a un servidor, poden arribar a saturar-lo, fer que no pugui lliurar-la i que quedi fora de servei. Això és un DDoS i avui en dia molts els fan pirates informàtics o màfies organitzades que controlen xarxes de milers d'ordinadors anomenades 'botnets'.

No és que aquests pirates informàtics tinguin moltes màquines a casa: aprofiten ordinadors de víctimes que es connecten a internet amb el Windows sense actualitzar, que no tenen tallafocs o antivirus o que fan servir programes amb problemes de seguretat. Els ciberdelinqüents fan servir aquestes fallades per infectar el ordinadors amb programes malignes que els permeten prendre'n el control i fer-los servir per fer aquesta mena d'atacs. Aquests ordinadors infectats s'anomenen 'zombies' perquè actuen sense que el propietari legítim s'adoni del que fan. Algunes 'botnets' en tenen milers sota control.

Trobar el responsable

Si l'atac va ser un DDoS amb ordinadors 'zombies', Castellano i Domingo-Ferrer admeten que serà difícil demostrar tècnicament qui ha encarregat l'atac. Castellano apunta que, en aquests casos, acostuma a funcionar millor investigar les xarxes socials i seguir vies d'investigació convencionals, no informàtiques, partint de la pregunta: a qui li interessava fer l'atac? El Govern té en compte que les webs dels Ferrocarrils de la Generalitat de Catalunya i de Transports Metropolitans de Barcelona ja van patir atacs semblants l'Onze de Setembre, per tant ja té un precedent, i afegeix que qui va fer el ciberatac té contactes al món de la ciberdelinqüència internacional. A més, avisa que un atac d'aquesta mena es pot considerar un delicte de danys penat amb entre sis mesos i tres anys de presó. "El volum dels atacs va ser tan gran, tan desconegut, que tenim l'obligació d'investigar i defensar-nos", ha declarat aquest dimarts al migdia el president Mas.

El Govern considera que l'atac de dissabte va ser, sobretot, una prova per comprovar els sistemes de la Generalitat i preparar l'envestida més contundent del diumenge. Però com que l'alarma ja va saltar dissabte l'endemà ja s'havia reforçat la seguretat, bloquejant el trànsit sospitós i canviant les rutes de comunicació internes per fer més difícils els atacs. Tot i amb això aquest primer assalt ja va afectar a fons els recursos digitals del Govern: les webs principals, el correu electrònic, el butlletí oficial i, sobretot, les receptes electròniques i l'accés als historials clínics van deixar de funcionar durant unes hores, ben bé fins a les sis de la tarda. I això que era d'esperar que, el cap de setmana del 9-N, hi hagués un atac informàtic d'aquesta mena. Castellano apunta que en aquests casos val la pena prevenir i que és molt important el temps de reacció per fer que les conseqüències de l'envestida durin tan poc com sigui possible.

Desinformació

A banda d'aquesta mena d'atacs el 9-N ja va patir obstacles d'una altra mena a través d'internet. Els últims, el cap de setmana passat mateix. Eren correus electrònics on s'anunciaven falses divisions dins l'ANC (https://twitter.com/esolert/status/531036607781298176) o fins i tot una també falsa dimissió de Carme Forcadell (https://twitter.com/oriolpineiro/status/531379743594401792) i que es van denunciar via Twitter. A l'octubre una campanya falsa anomenada Sign-in Catalunya (http://www.ara.cat/xarxes/campanya-Sign-in-Catalunya-electronic-unionista_0_1238276419.html) intentava aconseguir dades d'independentistes però es difonia des del correu electrònic de la web unionista xenòfoba.