Virus per a fer de soldats

L'Stuxnet, un virus informàtic de nova generació, podria haver afectat els sistemes de control del programa nuclear iranià. Els experts asseguren que això només pot ser obra de països amb recursos i amb una motivació clara, com ara els Estats Units o Israel.

La ciberguerra ha començat. Molts experts en seguretat mundial asseguren des de fa temps que en el futur les guerres es lliuraran, en gran part, a través dels ordinadors. Els darrers dies, l'Stuxnet, el virus informàtic més sofisticat dissenyat fins avui, els ha donat la raó. "Ens trobem en el mateix punt on érem quan es va inventar l'aviació. En aquell moment fou inevitable que algun científic treballés per trobar la manera d'utilitzar els avions per llançar bombes. Ara, els exèrcits tenen la capacitat de llançar una guerra cibernètica", assenyalava fa poc James Lewis, investigador del Centre per als Estudis Estratègics i Internacionals (CSIS), amb seu a Washington, en unes declaracions fetes al diari britànic *The Guardian*.

L'Stuxnet és el primer virus informàtic que ha estat dissenyat per sabotejar els sistemes de control de grans infrastructures, com, per exemple, embassaments, indústries petroquímiques o centrals nuclears. Aquest virus, de fet, ataca els sistemes anomenats SCADA, fabricats per l'empresa alemanya Siemens, que normalment es fan servir per controlar aquesta mena d'indústries. És per això que l'Stuxnet no s'expandeix per internet –perquè la majoria d'aquestes infrastructures no hi estan connectades–, sinó a través de dispositius USB. Un cop el sistema s'ha infectat, el virus intenta establir una comunicació amb un ordinador extern, des del qual es pot obtenir informació sobre la infrastructura que ha patit l'atac o, directament, sabotejar-la. Una de les principals característiques d'aquest virus és que respon a unes ordres molt precises i només s'activa en el cas de localitzar el component principal del sistema SCADA. L'empresa Siemens ha reconegut que almenys quinze empreses d'arreu del món han detectat la presència de l'Stuxnet als seus ordinadors, tot i que assegura que les seves funcions no van resultar afectades en absolut, perquè no eren l'objectiu per al qual el virus havia estat programat.

Per tot plegat, els experts consideren que la irrupció de l'Stuxnet posa de manifest l'inici d'una nova era en la guerra cibernètica. Segons Eugene Kaspersky –cofundador d'una empresa de productes antivirus–, aquest atac implica un punt d'inflexió. "Aquest programa no ha estat dissenyat per robar diners, enviar *spam* o aconseguir dades personals, sinó per sabotejar plantes i fer mal a sistemes industrials. Em temo que ens trobem davant l'inici d'un nou món. Els 90 foren la dècada del vandalisme cibernètic, el 2000 van arribar els criminals cibernètics i em fa l'efecte que ara ve l'era de les ciberguerres i del ciberterrorisme", assenyalava la setmana passada Kaspersky, en un comunicat. Segons ell, l'Stuxnet és tan sofisticat que, tot i que no hi ha proves per a identificar-ne els creadors, només pot haver estat desenvolupat per un equip molt ben preparat i amb molts mitjans econòmics, "probablement amb un estat al darrere". L'opinió de Kaspersky fou corroborada, segons que recollia l'agència Reuters, per Mikka Hypponen, cap de l'equip de recerca de l'empresa finlandesa F-Secure, que considera una cosa òbvia que l'Stuxnet "ha estat fabricat per un grup amb un gran suport tecnològic i financer".

EFE

Un equip de tècnics russos i iranians treballen en la construcció del reactor nuclear de

Infecció mundial. Els primers de detectar l'Stuxnet, el mes de juny passat, foren els tècnics de l'empresa bielorussa VirusBlokAda, quan provaven de resoldre un problema informàtic als ordinadors d'un dels seus clients, establert, curiosament, a l'Iran. Però no fou fins a final del mes passat que la premsa internacional es va fer ressò d'un problema informàtic a escala mundial que havia afectat, en la major part, l'Iran. Segons un estudi de l'empresa Symantec, l'Stuxnet va infectar més de 60.000 ordinadors en aquest país, uns 13.000 a Indonèsia, uns 6.000 a l'Índia i uns 3.000 als Es-

la central de Bushehr, a l'Iran. La imatge, sense data, ha estat facilitada per l'Agencia Atòmica Iraniana.

tats Units, com també, en menor mesura, aparells instal·lats en uns altres països. D'aquesta manera, la majoria de mitjans van apuntar cap al programa nuclear iranià –i, en concret, les centrals de Natanz i Bushehr– com a objectius més probables de l'Stuxnet. Segons alguns experts, el retard amb què ha ensopegat l'engegada de Bushehr i el mal funcionament d'un gran nombre de les centrifugadores que s'han instal·lat a la central de Natanz són una prova de l'èxit de l'Stuxnet. El pas següent, gairebé inevitable, ha estat identificar els responsables més probables del disseny d'aquesta arma cibernètica: els Estats Units i Israel, els dos països més interessats a impedir que l'Iran aconsegueixi la tecnologia necessària per a fabricar una bomba atòmica. Alguns experts, de fet, han apuntat l'anomenada Unitat 8200, una secció de l'exèrcit israelià especialitzada en codis informàtics, com a responsable del disseny de l'Stuxnet. En aquest sentit, fa uns dies el diari *The New York Times* recollia l'opinió d'un ex-membre dels serveis d'intel·ligència dels Estats Units, del quan no deia el nom, que implicava la Unitat 8200 en la lluita d'Israel contra la proliferació nuclear a l'Orient Mitjà. Segons aquest diari, l'any 2007 aquesta unitat va neutralitzar els radars de Síria i d'aquesta manera va facilitar l'atac de l'aviació israeliana contra una suposada central nuclear que es construïa en aquell país.

Sigui com vulgui, el fet és que, els darrers dies, el nom de Stuxnet ha inundat tots els debats sobre seguretat informàtica del planeta. A la conferència anual del Virus Bulletin, que es va fer a final de setembre a Vancouver, al Canadà, en què van participar les principals empreses fabricants de productes antivirus d'arreu del món, l'Stuxnet fou el protagonista indiscutible. Liam O Murchu, investigador de l'empresa nord-americana Symantec, va fer una demostració de com funciona aquest virus i de què és capaç de fer. A més, O Murchu va anar més enllà i va assegurar haver trobat un rastre en l'Stuxnet que el relaciona amb Israel. En concret, la xifra 05091979, que remet a la data del 9 de maig del 1979, dia de l'execució de Habib Elghanian, el líder de la comunitat jueva de l'Iran, que fou acusat de treballar per a Israel poc després de triomfar la revolució iraniana. Teories conspiratives a banda, segons el tècnic de Symantec el fet que l'Iran hagi estat el país més afectat per l'Stuxnet indica que aquest n'era l'objectiu.

Mentrestant, el govern de Teheran ha descartat la possibilitat que l'Stuxnet hagi afectat cap de les seves centrals nuclears. Així i tot, el 29 de setembre passat el cap de l'Agència Atòmica Iraniana, Ali Akbar Salehi, va reconèixer que havien detectat aquest virus en alguns ordinadors portàtils dels treballadors de la central de Bushehr, però va negar que el programa nuclear hagués quedat malmès. "Els nostres enemics han fracassat a l'hora de voler fer mal al nostre programa nuclear amb virus informàtics. Malgrat els seus esforços, tots els sistemes són completament nets", va assegurar Salehi, segons que recollia *The Guardian* l'endemà. En la mateixa edició, aquest diari recollia l'opinió d'Alan Bentley, de l'empresa de seguretat informàtica Lumension, segons el qual hi ha evidències que suggereixen que l'Iran era l'objectiu de l'Stuxnet, com ara el fet que "el virus fos identificat per una empresa bielorussa que treballa per a un client iranià; o que la planta de Bushehr no hagi treballat correctament durant mesos".

Tecnologia alemanya. La central nuclear de Bushehr és un projecte que fa més de trenta anys que s'arrossega. Es va començar a construir els anys 70 i hi van participar un grup d'empreses alemanyes, entre les quals hi havia, precisament, Siemens. Després d'un

EL TEMPS

El president iranià, Mahmud Ahmadinejad, durant una visita a la central nuclear de Natanz, l'abril del 2008.

parèntesi motivat per la revolució iraniana, el projecte va rebre un nou impuls l'any 1992, amb la signatura d'un acord entre l'Iran i Rússia. Tot i que Siemens ja fa anys que es va retirar del projecte, les empreses russes que han desenvolupat el nou programa nuclear iranià han continuat utilitzant components i tecnologia fabricada per aquesta empresa alemanya. Es tracta, sens dubte, d'una altra evidència –com han assenyalat els experts– que l'objectiu de l'Stuxnet era l'Iran.

De fet, tot i que la central nuclear de Bushehr fou inaugurada oficialment el mes d'agost d'enguany, se n'ha retardat novament l'engegada. El 30 de setembre proppassat la cadena BBC recollia unes declaracions d'Ali Akbar Salehi, cap del projecte atòmic iranià, en què deia que el procés de càrrega de combustible de la central de Bushehr es completarà el mes de novembre, però que l'inici de la producció elèctrica i la connexió amb la xarxa no es farà fins el gener de l'any que ve, és a dir, dos mesos més tard de la data prevista. Amb tot, Salehi va assegurar que aquest retard no ha tingut res a veure amb cap virus informàtic, tot i que, segons que assenyalava la BBC, no va donar cap més explicació. Al seu torn, el ministre d'Afers Estrangers iranià, Ramin Mehmanparast, va negar totes les informacions publicades per la premsa internacional que relacionen l'Stuxnet amb aquest retard, i les va qualificar de propaganda i de formar part d'una "guerra encoberta" contra l'Iran. "La planta de Bushehr progressa d'acord amb el calendari establert", va declarar Mehmanparast a l'Agència Iraniana de Notícies. Igualment, el sots-president de l'Agència Atòmica d'aquest país, M. Zarean, va assegurar que s'havien pres tota mena de mesures per evitar atacs cibernètics contra les instal·lacions nuclears.

Sigui com sigui, alguns experts consideren que el risc d'una guerra cibernètica és més petit ara que no pas abans de la irrupció de l'Stuxnet, precisament pel fet que l'element sorpresa ha desaparegut. En aquest sentit, tal com recollia una opinió publicada pel setmanari *The Economist* a l'edició de la setmana passada, l'Stuxnet ha mostrat les limitacions de la ciberguerra perquè, segons que sembla, l'atac del virus només ha reeixit a endarrerir el programa nuclear iranià, però no pas destruir-lo. Segons aquest setmanari, l'Stuxnet ha servit, si més no, per a soscavar la idea que occident és més una víctima potencial d'un atac cibernètic que no el responsable. Passa, advertia *The Economist*, que en aquesta mena de batalla mai no se sap amb claredat qui ataca qui i, sobretot, si al cap i a la fi l'atac ha tingut èxit o si, per contra, ni tan sols ha existit.

Xevi Camprubí