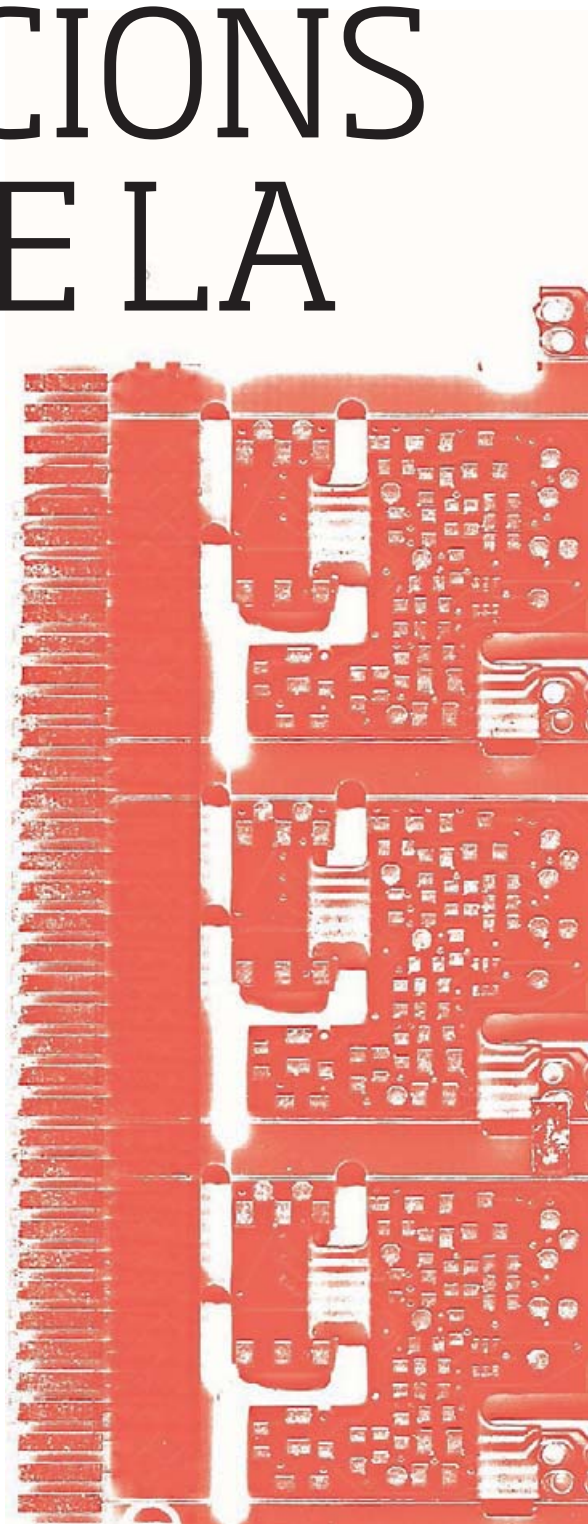
LES APLICACIONS SECRETES DE LA POLICIA

La lluita contra els cibercrims compta amb cada cop més ginys per assegurar la vigilància gairebé total

TEXT__**GINA TOST / XAVIER VIDAL**



A 'BLACKHAT', LA PEL·LÍCULA DE MICHAEL MANN estrenada aquest any sobre el món del ciberterrorisme, el protagonista Nick Hathaway (Chris Hemsworth) aconsegueix accedir il·legalment a una eina informàtica exclusiva anomenada Black Widow, que només té l'Agència de Seguretat Nacional (NSA) nord-americana. L'objectiu és recuperar la informació d'un disc dur que ha quedat totalment destruït per l'explosió d'un reactor nuclear provocada pels terroristes cibernètics. ¿Existeix realment aquesta eina o aplicacions semblants que només tenen les policies? ¿De quins altres instruments, més o menys secrets, disposen les policies d'arreu del món per combatre l'acció dels delinqüents digitals del segle XXI?

Black Widow existeix i no és, ni de bon tros, l'única navalla suïssa secreta al món digital de les ciberpolicies. A principis de juliol l'exanalista de la CIA Edward Snowden va filtrar informació detallada sobre un programa informàtic anomenat XKeyscore, d'ús exclusiu de la NSA i que ho pot esbrinar gairebé tot de nosaltres. Ho fa capturant el trànsit dels nostres ordinadors i dispositius mòbils a través d'internet i emmagatzemant tot el que fem, com ho fem i quan ho fem. Curiosament, en els mateixos dies, l'empresa italiana de seguretat informàtica Hacking Team va patir una intrusió en els seus sistemes, amb el robatori de gairebé 400 gigabytes d'informació confidencial. Aquesta empresa es dedica, entre altres coses, a fabricar virus i programari maliciós per a nombrosos governs i agències de seguretat d'arreu del món, inclòs el servei d'espionatge espanyol, el CNI, segons consta en la documentació filtrada sobre Hacking Team i segons va reconèixer la mateixa agència en diversos mitjans de comunicació. El programari maliciós que subministra aquesta companyia és absolutament exclusiu i serveix per prendre el control d'ordinadors de manera remota sense que el propietari n'estigui al cas.

EL BLACK WIDOW

Les policies i agències de seguretat arreu del món fan servir instruments gairebé inimaginables per a l'usuari mitjà. El Black Widow que apareix a la pel·lícula de Michael Mann no és, en realitat, un programa, sinó un superordinador amb una capacitat d'anàlisi de dades espectacular, instal·lat originàriament a Fort Meade, a l'estat nord-americà de Maryland. Abraham Pasamar, director executiu de l'empresa de seguretat informàtica INCIDE, creu que aquest supercomputador pot ser "l'encarregat dels processos d'intel·ligència, una cosa semblant al gran cervell d'un nou Echelon [la gran xarxa secreta d'espionatge a l'Europa preinternet]". Amb aquest poder de procés, la recuperació d'informació esborrada o destruïda o la desencriptació de fitxers per la força, per exemple, són molt més ràpides i eficaces. A Espanya, la Policia Nacional també recorre a superordinadors per analitzar dades informàtiques que puguin menar a la detenció dels criminals. Isidro Ordás, cap de la secció de delictes tecnològics de la Policia Nacional, assegura: "A Espanya comptem amb computadores com el MareNostrum", de la UPF de Barcelona, amb qui tenen "acords de col·laboració" i que es pot fer servir en processos d'investigació judicial.

XKEYSCORE, EL GRAN GARBELL

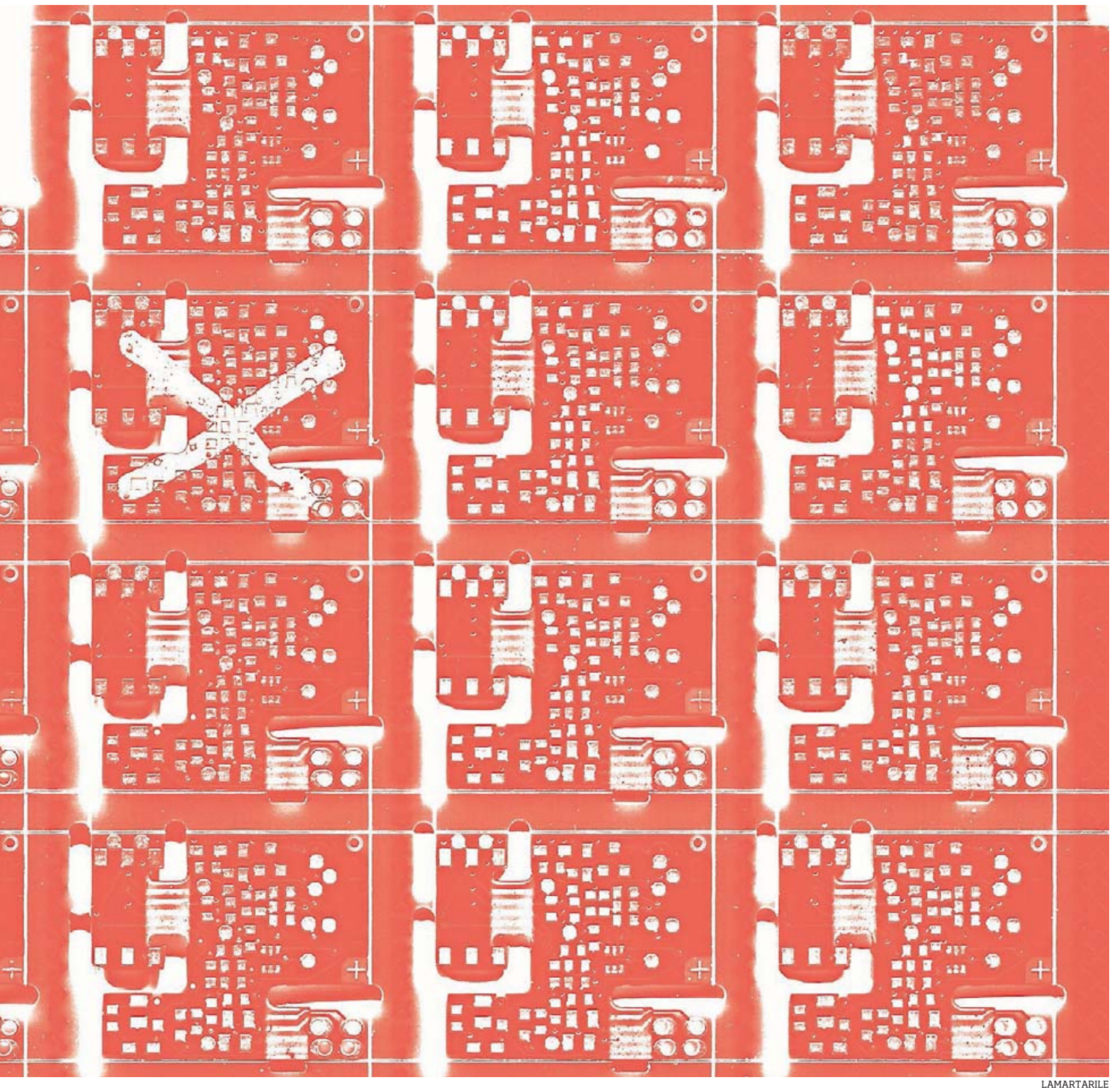
Una de les eines més desconegudes fins que Edward Snowden va publicar el seu manual d'ús és el programa XKeyscore. Es tracta d'un motor de cerca d'un abast tan descomunal que gairebé ho pot esbrinar tot de nosaltres. John Adams, ex cap de seguretat i operacions de Twitter, explica que l'aplicació "monitoritza el trànsit i la recollida de dades privades de persones o organitzacions concretes". En la pràctica, es tracta d'una xarxa de més de setcents servidors distribuïts en països arreu del món –Espanya inclosa, segons el manual d'ús filtrat a Wikileaks–, que poden capturar i processar les dades que circulen per internet, endreçar-les i classificar-les per ser consultades remotament pels agents de la NSA.

El sistema té establerts diversos criteris de classificació d'informació per defecte. Per exemple, si algú fa una cerca al seu mòbil, ordinador o tauleta en àrab a Alemanya, XKeyscore ho detecta, captura la cerca i la guarda: qui l'ha feta, des de quin ordinador i tota la resta de dades rellevants. O si algú fa servir encriptació per enviar un correu electrònic o fa una cerca de determinades paraules considerades sensibles, el mecanisme es posa en marxa i emmagatzema la informació potencialment *perillosa*. Es tracta del més semblant al Gran Germà d'Adolf Huxley. En el fons, XKeyscore representa un canvi d'eix en el seguiment del ciberdelicte. No es tracta d'intervenir les comunicacions d'un sospitós, amb autorització o sense, amb un objectiu concret, sinó d'una observació a l'engròs per detectar possibles comportaments irregulars. Segons diversos càlculs, alguns d'aquests servidors, aquests enormes garbells digitals, poden arribar a capturar més de vint terabits en un sol dia, un volum d'informació equivalent a més de cinc milions de cançons o tretze mil pel·lícules. Qualsevol agent de la NSA pot accedir remotament a aquesta informació sense haver de sol·licitar prèviament el permís d'un jutge.

Més enllà de les implicacions morals sobre la possible vulneració de la privacitat, John Adams posa també l'accent en el fet que el programa no és gaire segur. "Per exemple, el sistema d'accés sí que registra qui fa la consulta, però, en canvi, les bases de dades en si no tenen aquest control", reflexiona. Això significa que qualsevol podria connectar-se directament a les bases de dades, esbrinar informació sensible i no deixar rastre de la consulta. Adams afegeix que "ja hi ha hagut casos dels mateixos empleats de la NSA que han accedit il·legalment a l'aplicació per consultar dades sobre amics o coneguts". Aquesta pràctica fins i tot té un nom: *loveint*. Per als usuaris amb accés a aquest programari, "la temptació d'usar-lo sense deixar rastre és molt gran", conclou Adams. De fet, la senzillesa de funcionament d'una eina tan poderosa com XKeyscore ha fet que molts analistes l'hagin batejat com "el Google de la policia".

ACCÉS LLIURE PER A PARTICULARS

Ara bé, no cal ser policia per accedir a aplicacions poc conegudes però molt potents que permeten entrar, per exemple, a les dades dels dispositius mòbils d'una altra persona a través de la còpia guardada al núvol i sense necessitat de la seva contrasenya. El programa Elcomsoft Phone Breaker, de venda legal a través d'internet, promet fer-ho a preus que van dels 79 als 799 dòlars i està a l'abast de qualsevol particular o empresa. Nicolás Castellano explica que es tracta d'una "eina comercial que es ven a particulars i a empreses i que té una versió Forensic que pot accedir a informació de terminals mòbils d'Apple i BlackBerry i a informació de l'iCloud i Windows Live per obtenir les dades guardades al núvol". La majoria d'aquestes marques de telefonia ja inclouen en els seus models la còpia de seguretat de les nostres dades en servidors remots. Castellano diu que per obtenir aquesta informació "n'hi ha prou acce-



LAMARTARILE

dint a l'ordinador des del qual s'ha entrat a iCloud i obtenir les dades temporals de validació". Tot i que el mercat d'aquest tipus de productes és completament obert, Nicolás Castellano diu que "els cossos policials poden accedir a descomptes, mòduls de programes o maquinari específic per desprotegir programari o mòbils que normalment no és ofert a empreses consultores o particulars". "És una pràctica molt de moda que prové dels EUA", assegura. De tota manera, continua Castellano, "l'única limitació que tenen alguns cossos policials avui dia per poder adquirir aquest tipus de productes és econòmica", tot i que a l'hora de fer-les servir, òbviament, cal l'ordre judicial corresponent.

MÉS CONTROL A EUROPA

A Europa, aquest control judicial de les eines d'anàlisi informàtica policial és molt més estricte. La Policia Nacional, per exemple, fa servir un programari d'anàlisi forense anomenat Encase, segons reconeix Isidro Ordás. Aquest programa permet la clonació de qualsevol dispositiu mòbil o de sobretaula: en crea una imatge perfecta sobre la qual es pot treballar. El programa extreu de la còpia tota la informació emmagatzemada, des de correus electrònics fins a pàgines d'internet visitades, documents ofimàtics o converses de xat, segons explica la mateixa empresa creadora a la seva web. Fins i tot si l'usuari ha esborrat, amagat o camuflat aquesta informació, el programa és capaç de trobar-la, reconstruir-la i indexar-la per ser usada en processos judicials.

Al marge de l'anàlisi forense, a casa nostra les forces de seguretat disposen de dos sistemes regulats legalment però gairebé secrets que permeten intervenir les comunicacions d'un presumpte delinqüent. Es tracta del Sitel, utilitzat per les forces de seguretat espanyoles, i el Siltec, una versió modificada però amb un funcionament semblant que fan servir els Mossos d'Esquadra. Una vegada autoritzades per un jutge, aquestes eines tenen la capacitat de connectar-se amb les empreses de telefonia i enregistrar les comunicacions de les persones que estan sent investigades. Ara bé, com que les comunicacions a través de mòbil van xifrades, les empreses telefòniques han de subministrar a les policies la corresponent clau de xifratge per poder accedir al contingut de converses o trànsit de dades.

VIRUS PER A L'ACCÉS REMOT

De moment, l'ús de les eines d'extracció d'informació està restringit a dispositius que la policia tingui físicament als seus laboratoris i hagin sigut obtinguts sota el paraigua d'una ordre judicial, però les possibilitats d'accés remot a mòbils o ordinadors són molt grans. Abraham Pasamar reconeix que "aquest tipus d'accés ara mateix no està previst, però hi ha un debat molt viu sobre el tema". Isidro Ordás hi coincideix quan afirma que aquesta via de la intervenció remota mitjançant programari maliciós "està sent debatuda en l'actualitat com una de les possibles incorporacions a la nostra llei d'enjudiciament criminal". En qualsevol cas, sempre s'aplicaria en delictes greus i sota un control complet d'un jutge. Però ja hi ha països que fan servir aquest sistema.

De fet, l'ús de virus en forma de troians o programari maliciós per part de les autoritats només està previst en la legislació alemanya. El 2007 l'estat de Rin del Nord - Westfàlia va aprovar una normativa que permetia a la policia l'ús de troians, però el 2008 el Constitucional va restringir la llei i ara només es pot aplicar en casos de possible terrorisme.

El ventall d'actuacions policials contra els ciberdelinqüents amb un recurs permès per la llei, com ara la infecció remota d'ordinadors, és amplíssima. John Adams, ex cap de seguretat i operacions de Twitter, explica: "Empreses com Gamma International i Hacking Team ho han fet i ho continuen fent: ofereixen armes de *malware* que es poden dirigir contra ciutadans corrents". Segons Adams, "aquest programari maliciós ataca l'usuari i instal·la eines, conegudes com a RATS (eines d'accés remot), que permeten prendre el control i tenir accés complet a l'ordinador de la víctima, incloent-hi la càmera de vídeo o el micròfon". Ara mateix, aquest tipus de programari secret ja el fan servir molts governs arreu del món.

Gràcies a una filtració de Wikileaks es va saber que governs com ara Qatar, Sud-àfrica, Austràlia i Itàlia, per citar-ne només uns quants, fan servir un programa anomenat FinFisher, creat per l'empresa alemanya Gamma Group. Castellano explica que es tracta d'una aplicació "de vigilància que enregistra totes les comunicacions d'un ordinador o mòbil prèviament compromès". Les dades revelades per Wikileaks indiquen que la companyia podria haver ingressat entre cinquanta i cent milions d'euros en la venda d'aquest programari.

El FinFisher pot capturar des del correu electrònic fins a les videoconferències o el que capta la càmera o el micròfon del dispositiu. La infecció d'ordinadors o dispositius mòbils sol ser un pas previ per instal·lar totes aquestes aplicacions desconegudes que permeten enregistrar qualsevol pas que es faci en els nostres aparells. De fet, el programa FinFisher ha sigut denunciat per activistes socials i fins i tot per empreses com ara Mozilla, que el 2013 va informar que aquesta apli havia suplantat una de les extensions del navegador Firefox per infectar els ordinadors que se l'instal·laven.

TORRES DE COMUNICACIÓ FANTASMA

Les eines més o menys secretes que s'usen arreu del món no sempre són programari. John Adams explica un exemple absolutament desconegut per la majoria de ciutadans. "És un dispositiu conegut com a Stingray, que sembla una torre de telefonia cel·lular i permet gravar dades de veu, copiar textos i totes les dades que es mouen a través dels telèfons específics", assegura. De moment, tot el que envolta aquestes torres de comunicacions situades als EUA i la Gran Bretanya és un misteri. Ara mateix hi ha batalles en curs per obligar el fabricant a revelar com funcionen els dispositius Stingray. Aquests ginys han sigut creats per un important contractista de defensa nordamericà que obliga els compradors a firmar un contracte de confidencialitat. Sigui qui sigui que els instal·la i fa servir, per a John Adams "són altament invasius i nocius per a la privacitat". Per sort, a casa nostra encara no existeixen aquestes torres de comunicacions secretes i falses.

Sigui com sigui, la realitat és que no tan sols les autoritats tenen accés a tot aquest ventall d'eines més o menys secretes o desconegudes. El mercat de venda és comú per a les policies que volen fer complir la llei i per als ciberdelinqüents que volen saltar-se-la. I no sempre està clar qui va per davant en aquesta cursa. Adams creu que "la majoria de les forces de l'ordre estan molt per darrere dels criminals, perquè no estan acostumades a tractar amb aquest tipus de problemes de seguretat i la tecnologia es mou més ràpid que la policia, que no pot mantenir el ritme". Per sort, l'acció de la policia és cada vegada més ràpida i més eficaç en la cursa per atrapar els ciberdelinqüents i, fins i tot, preveure els ciberdelictes. ■