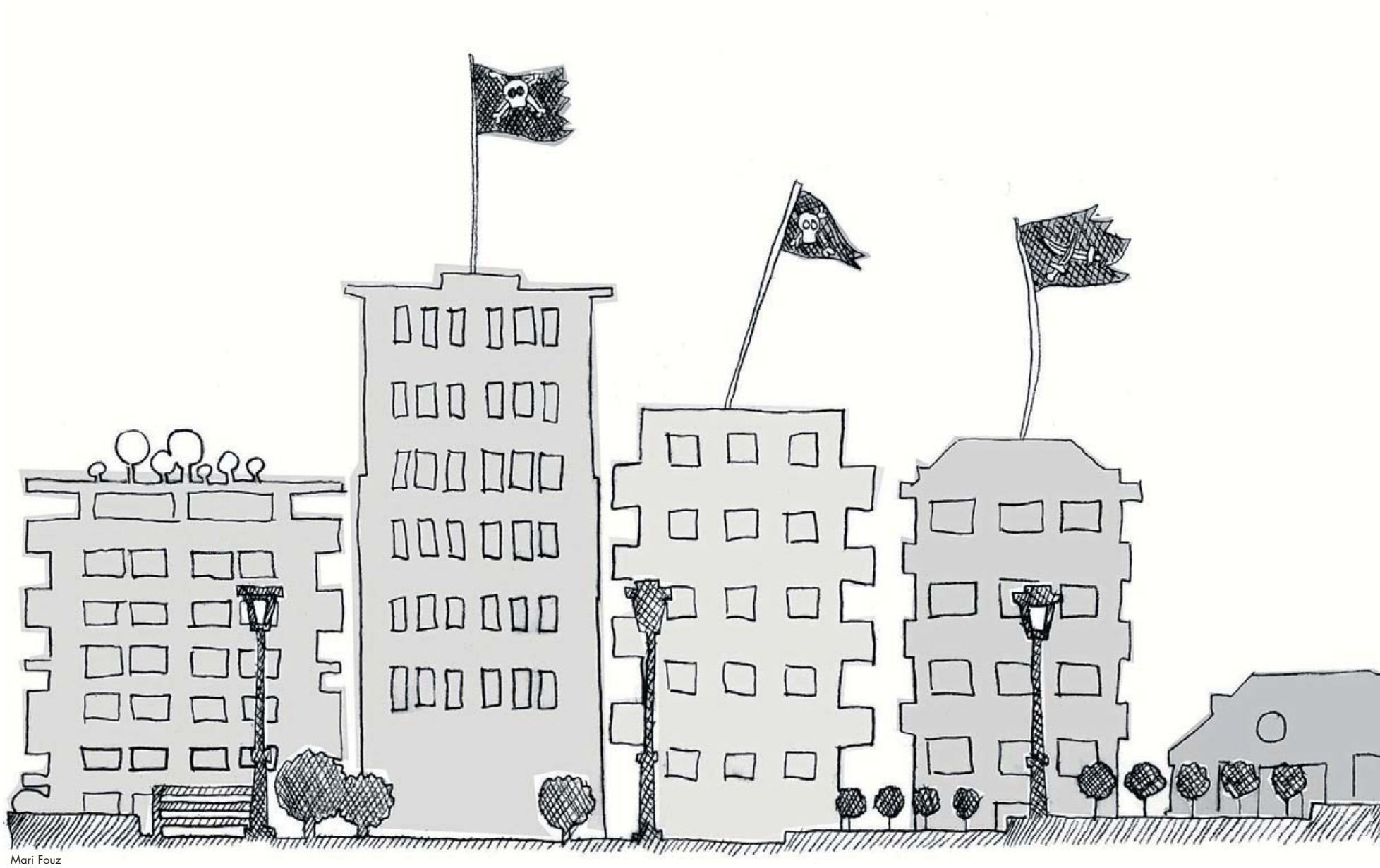
LA CIUTAT MÉS PERILLOSA A INTERNET

Ramnicu Valcea, a Romania, és coneguda per l'FBI amb el nom de Hackerville per la gran quantitat de delictes cibernètics de tot tipus, des d'estafes fins a atacs dirigits, que hi tenen l'origen



Mari Fouz

TEXT
Xavier **Vidal** / Gina **Tost**

Un dels temes candents de la campanya electoral als Estats Units ha sigut el robatori de correus a la candidata demòcrata, Hillary Clinton. Els demòcrates van acusar Rússia d'estar al darrere de l'atac informàtic. Els informes sobre seguretat cibernètica situen Rússia com un dels focus de delinqüència electrònica més grans a escala mundial, juntament amb el Brasil, la Xina i el petit comtat romanès de Valcea. La capital d'aquest comtat, Ramnicu Valcea, d'uns cent mil habitants, és anomenada Hackerville per l'FBI pel gran nombre de delictes informàtics que hi tenen l'origen.

Els *hackers* dolents, que molts anomenen *black hats*, han deixat de ser llops solitaris devoradors de pizza i addictes als refrescos ensucrats com en els anys noranta del segle passat. En els últims temps els ciberdelinqüents s'han agrupat, s'han professionalitzat i s'han organitzat en focus concentrats especialment en algunes regions del planeta. El perfil de *hacker* solitari ha sigut substituït per un concepte anomenat FaaS, que significa *frau com a servei* (*fraud as a service*, en anglès).

El cas de la ciutat de Ramnicu Valcea és significatiu i il·lustra aquesta evolució. Després de la caiguda del líder comunista Nicolae Ceausescu l'any 1989 a Romania es van obrir moltes portes, i una de les més esperades va ser la de la tecnologia. Un bon nivell educatiu tecnològic i unes bones comunicacions digitals van convertir la informàtica en una gran oportunitat de negoci. A principis d'aquest segle a Ramnicu Valcea van multiplicar-se els cibercafès, amb connexions a internet relativament ràpides i molt barates. Les necessitats econòmiques d'una població que venia de la misèria comunista van servir de motor per convertir una petita i tranquil·la ciutat de l'interior de Romania en Hackerville. I molts ciutadans que tenien poques opcions laborals de guanyar-se la vida en altres àmbits es van posar a treballar en la indústria del frau. Luis Corrons, director tècnic de Panda Lab, creu que és un exemple semblant al de Rússia. En un altre país els joves "estarien treballant en multinacionals tecnològiques, però com que a Rússia no tenen oportunitats, molts d'ells opten per aquesta solució, que els permet guanyar molts diners" sense moure's del seu lloc d'origen.

Mil milions de frau

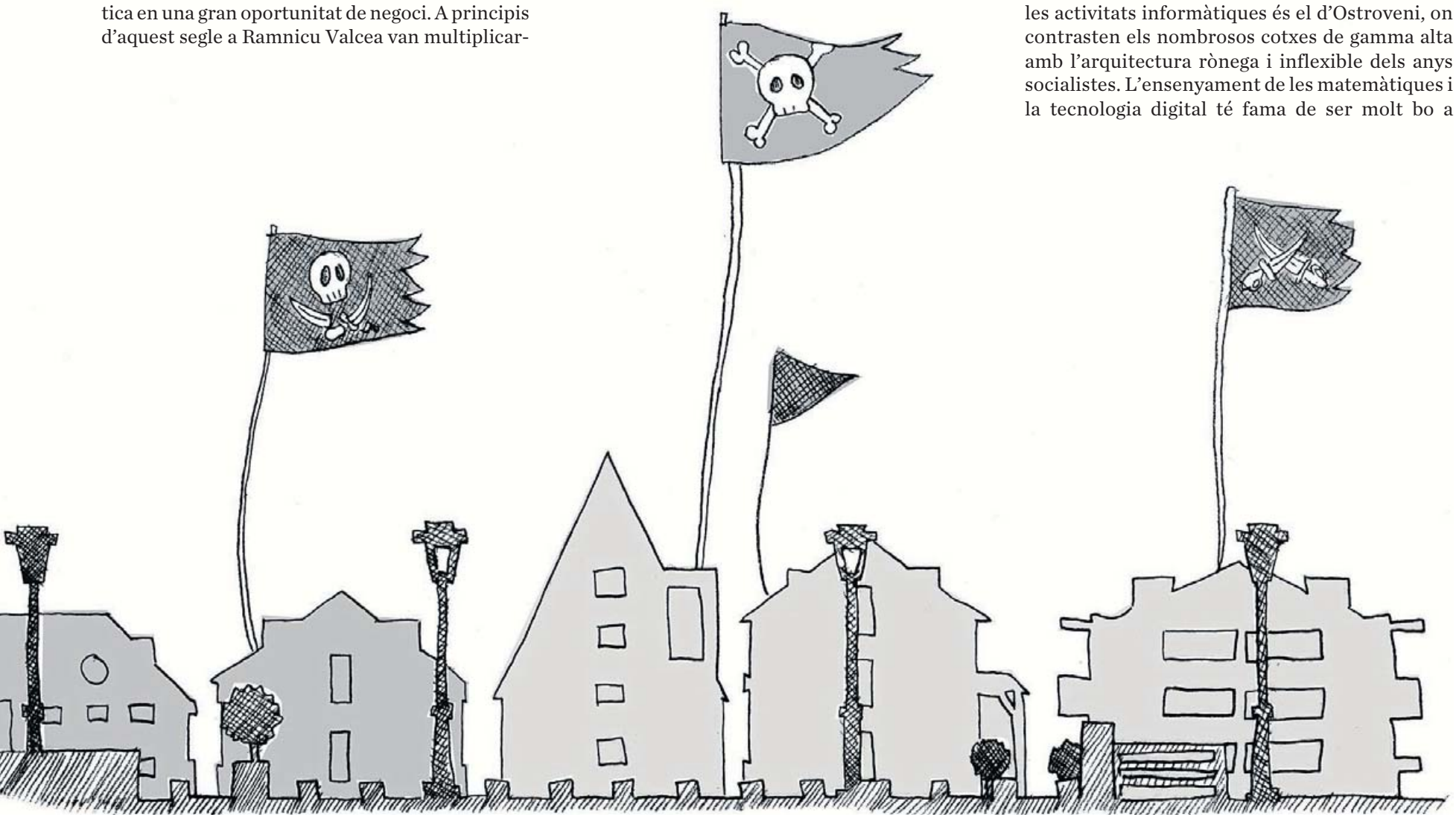
L'any passat, segons dades de l'empresa Norton, el frau a internet provinent de la zona de Romania rondava els mil milions de dòlars. I això només són les operacions de les quals es va poder esbrinar l'origen. Alberto Ruiz Rodas, enginyer de Sophos Iberia, explica que "des d'aquesta ubicació s'han llançat atacs a organismes molt coneguts, i un percentatge important dels seus habitants s'han guanyat o encara es guanyen la vida" amb aquest tipus de delictes informàtics.

Una dada significativa és que en una ciutat d'unes dimensions semblants a Reus hi ha una desena d'oficines de la Western Union, la multinacional d'enviament de diners arreu del món. Tot i que l'empresa no té res a veure amb les estafes, és un vehicle perfecte per portar-les a terme, perquè permet fer transferències de diners ràpides i amb un alt nivell d'anonimat. El sistema de fraus digitals necessita un intermediari. L'estafador demana a l'estafat que faci un ingrés a la Western en pagament per un determinat producte o servei. L'usuari se'n refia i paga pensant que s'està aprofitant d'una gran oferta o que guanyarà uns diners fàcils. L'estafador va a l'oficina i recull els diners que ha enviat l'estafat i mai més se'l torna a veure. Ni a ell ni al servei o producte que l'estafat ha comprat. La majoria de petites estafes de Hackerville han fet servir la Western com a intermediari. Aquests fraus són tan habituals que a la seva pàgina web l'empresa diu que no es fa responsable "de la qualitat dels béns o serveis rebuts, ni de la no recepció" del que es paga a través del seu sistema.

> *En una ciutat de la mida de Reus hi ha una desena d'oficines de la Western Union*

¿Com arriba una petita ciutat rural a ser el focus d'atenció de les policies d'arreu del món? És la conseqüència de la suma de molts factors. Valcea és un dels comtats més pobres de Romania: ocupa el lloc 21 de les regions romaneses per nivell de renda per càpita, però la xifra d'atur oficial és baixa, està al voltant del 5%. En contrast amb la pobresa de les estadístiques oficials, un informe de *Forbes* d'aquest mateix any situava Ramnicu Valcea entre les 25 millors ciutats de Romania per fer-hi negocis. Probablement la indústria del frau per internet hi té molt a veure.

Segons l'informe elaborat per l'empresa d'antivirus Norton, el districte on es concentren les activitats informàtiques és el d'Ostroveni, on contrasten els nombrosos cotxes de gamma alta amb l'arquitectura rònega i inflexible dels anys socialistes. L'ensenyament de les matemàtiques i la tecnologia digital té fama de ser molt bo a



Romania, i els joves aprenen a programar d'adolescents amb l'esperança de guanyar molt més que el salari mínim, que és de poc més de 200 euros al mes.

El problema de la delinqüència electrònica a Ramnicu ha arribat fins i tot a l'Església, i a YouTube es poden trobar vídeos de sacerdots de la ciutat que demanen als feligresos que no segueixin els models d'alguns *hackers* dolents que s'han convertit en icones per a molts joves. Un exemple clar és Nicolae Popescu, un delinqüent informàtic que està inclòs a la llista dels més buscats de l'FBI i pel qual l'agència nord-americana ofereix una recompensa d'un milió de dòlars. Popescu operava des de Hackerville i l'FBI fa quatre anys que el busca per frau electrònic, blanqueig de diners i tràfic de marques i serveis falsos. L'acusa d'haver estafat vora un miler d'usuaris amb vendes falses de cotxes, vaixells, propietats i molts altres béns i serveis.

Especialització regional

Més enllà de Hackerville, la delinqüència digital organitzada segons el model FaaS ha tendit a concentrar-se els últims anys en determinats països. L'informe de ciberseguretat de l'empresa Akamai, que dóna servei de transport de dades a internet a les principals companyies del món, cita el Brasil, la Xina i Rússia com tres dels principals focus del ciberdelicte. Dani Creus, analista de programari maliciós de Kaspersky Lab, opina que "una legislació inexistent o obsoleta, poca capacitat operativa policial per investigar delictes i la permissivitat de determinats governs poden alimentar aquests focus" de delinqüència digital.

A més, la situació en molts països del món dels grups de delinqüència electrònica organitzada és complexa. Els EUA han acusat alguns estats de ser massa permissius amb el frau electrònic, o directament d'instigar atacs informàtics, com ara la Xina i Rússia. El panorama canvia radicalment, però, quan hi ha cooperació entre estats. Dani Creus diu que els recents acords entre la Xina i els EUA, per exemple, "han provocat que col·laboradors civils es quedin sense el suport que els proporcionava el mateix govern quan feien operacions a petició seva". Això ha fet que alguns d'aquests grups "es dediquin a un altre tipus d'activitats, com ara el frau amb troians bancaris, extorsions mitjançant atacs DDoS o *ransomware*", explica. El *ransomware* és el segrest per encriptació dels arxius d'una empresa, que per poder-los tornar a fer servir ha de pagar un rescat al grup delinqüent que els ha encriptat.

Hi ha exemples de la relació d'alguns estats amb grups civils de *hackers*. Un d'ells el va publicar Kaspersky Lab quan va descobrir les afinitats entre l'Agència Nacional de Seguretat nord-americana (NSA) i l'Equation Group, una organització responsable de més de mig miler d'infeccions amb *malware* en 42 països arreu del món, tant a empreses privades com a agències estatals, o fins i tot dirigents polítics. Kaspersky va creuar la informació de què disposava sobre els codis maliciosos de l'Equation Group amb la informació publicada per l'exanalista de la CIA Eduard Snowden i va trobar proves que aquest grup havia sigut la mà d'obra especialitzada en delictes informàtics de la NSA durant més d'una dècada.

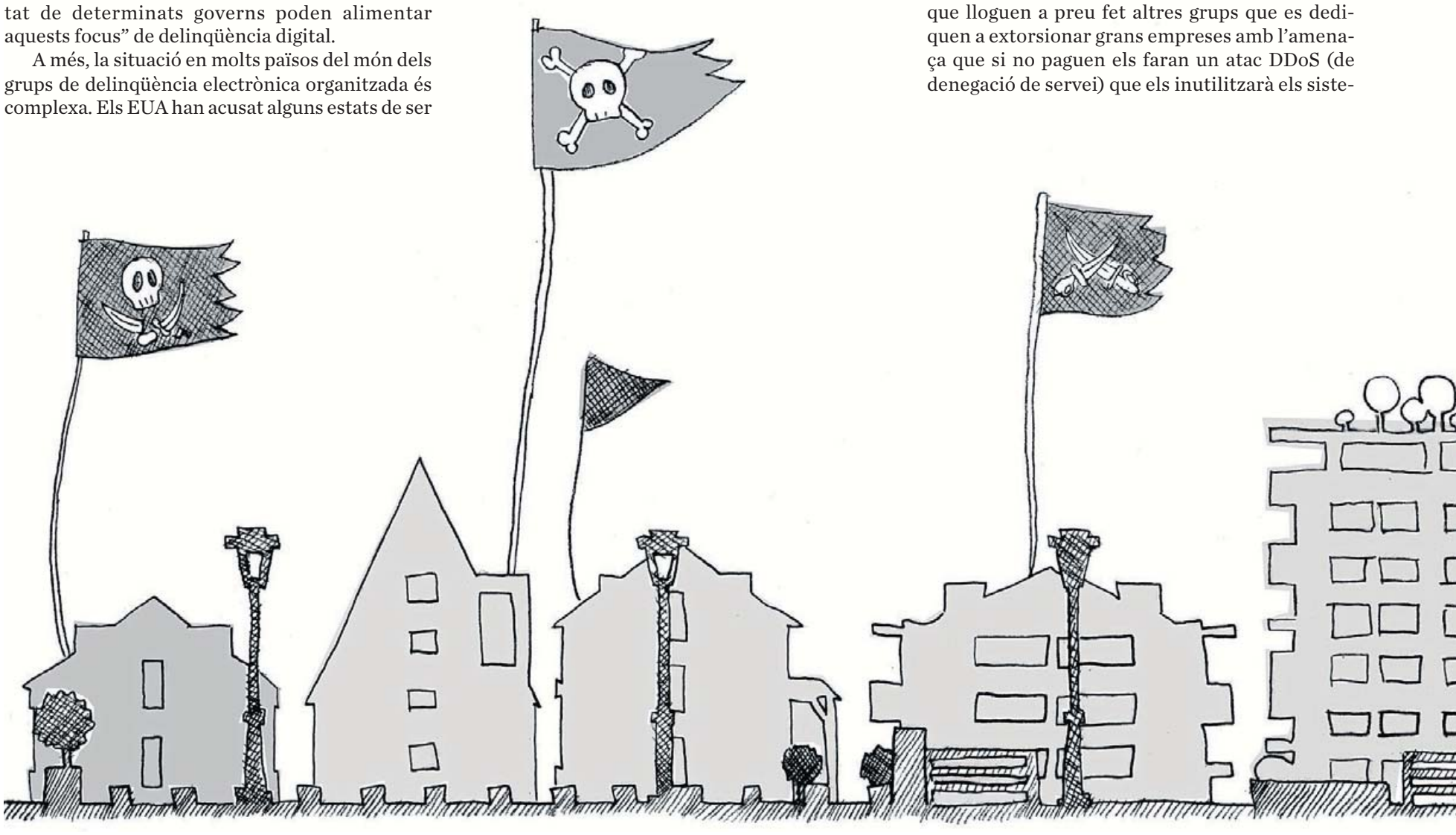
La venda de 'malware' aporta més beneficis que la d'armes il·legals

Lentament, alguns estats han començat a prendre's seriosament el frau per internet. Nigèria és un d'ells. Resulta curiós que la famosa enganyifa del nigerià que demana una petita quantitat de diners per diferents causes presumptament solidàries s'hagi convertit en "el frau 419", en referència a l'article del Codi Penal nigerià que ja castiga aquesta mena de delictes.

Especialització temàtica

El mercat del programari maliciós és tan rendible que s'ha organitzat en *multinacionals* que es dediquen de manera molt professional a crear *malware* per robar els diners als usuaris. O per fer servir els seus ordinadors particulars sense que se n'adonin en macrooperacions d'atacs de denegació de servei (DDoS) a grans empreses i organismes públics. Alberto Ruiz Rodas assegura que aquestes "multinacionals del *malware* facturen més diners a l'any que les dedicades a la venda il·legal d'armes al món".

Luis Corrons explica que s'organitzen en grups relativament petits especialitzats en tasques específiques del procés global. "Hi ha programadors que desenvolupen el programari maliciós, grups centrats a infectar ordinadors i d'altres encarregats de comercialitzar i monetitzar la informació robada", explica. Fins i tot n'hi ha que s'encarreguen de muntar xarxes d'ordinadors *zombis* (infectats pel programari maliciós) que lloguen a preu fet altres grups que es dediquen a extorsionar grans empreses amb l'amenaça que si no paguen els faran un atac DDoS (de denegació de servei) que els inutilitzarà els siste-



mes informàtics. L'exemple de col·laboració més recent és l'atac massiu del divendres 21 d'octubre contra l'empresa Dyn, que va comportar la caiguda dels serveis de Twitter, Spotify, Ebay i Github. El grup responsable de l'acció va alliberar al principal fòrum de *hackers* el codi de Mirai, el programa usat en l'operació DDoS contra Dyn, per aconseguir que altres col·lectius se sumessin a l'atac. I el resultat va ser l'amplificació massiva de l'acció, que va convertir gravadores de vídeo DVR, impressores i càmeres de seguretat en esclaus a les ordres dels ciberdelinqüents.

Fins i tot pot haver-hi col·laboració entre grups de delinqüència sobre el terreny i els del món virtual. Dani Creus pensa que "els grups que sempre han operat al món físic saben que internet és un mitjà excel·lent per dur a terme les seves activitats i seria ingenu pensar que no tinguin experts en matèria digital" dels nous grups cibernètics.

Com en el món dels negocis tradicionals, també hi ha rivalitats i guerres de preus entre els grups de ciberdelinqüència. A principis d'aquest any, IBM X-Force va descobrir un programari maliciós per a mòbils Android anomenat GM Bot. Era tan efectiu que els seus autors, que feien servir el nom de GranjaMan, van triplicar el preu del *kit* del programari maliciós dels cinc mil dòlars originals fins als quinze mil. Aquest increment indiscriminat de preu va provocar disputes amb alguns clients, que van protestar en els fòrums on es fan aquest tipus d'operacions fins al punt que GranjaMan va ser expulsat. De seguida tres *kits* més de *malware* d'altres autors van prendre el mercat: Bilal Bot, Cron Bot i KNL Bot, tots ells amb preus molt més econòmics que el de GranjaMan, que anaven entre els tres mil i els sis mil dòlars. Tots tres, a més, amb funcionalitats semblants a l'inflacionista GM Bot, com ara intercepció i enviament de SMS, indetectabilitat i control remot del mòbil, incloent-hi el bloqueig de telèfon i la manipulació del so i de la pantalla.

El divendres 21 d'octubre un atac massiu contra Dyn va fer caure Twitter

Dani Creus afirma que es tracta d'un "mercat relativament madur en què es pot trobar pràcticament tot el que es necessita per posar en marxa campanyes d'infecció massiva, operacions d'extorsió o blanqueig de diners", entre d'altres.

Preus variables

Els preus no sempre són estàndards i, com en el cas de l'economia clàssica, les circumstàncies marquen la cotització. Luis Corrons posa l'exemple de la Xina, on existeix un ecosistema bastant tancat. Allà, explica Corrons, "funciona la llei de l'oferta i la demanda, i com més delinqüents ofereixen un mateix programa, més baixa el preu, de manera que es busca la diferenciació aportant el valor afegit de la qualitat". Un exemple es va produir quan es va popularitzar el comerç de dades de targetes de crèdit o accés a comptes bancaris al mercat negre. Hi havia tanta oferta, segons Corrons, que el preu era molt baix, des d'un dòlar per número de targeta, i això va fer que alguns grups comencessin a oferir dades bancàries a preus més alts però garantint que els comptes disposaven d'un mínim de diners per ser robats.

Aquests grups funcionen com empreses i tracten de "maximitzar beneficis constantment millorant les seves capacitats de distribució de codis maliciosos o infraestructures", explica Dani Creus. Fins i tot hi ha casos de guerres entre aquests grups que han provocat atacs dels uns als altres, cosa que ha tingut com a resultat la filtració de dades molt interessants per a les autoritats, com ara bases de dades internes o codis font de *malware*. Luis Corrons té clar que es tracta d'organitzacions que "funcionen com autèntiques pimes, cadascuna especialitzada en el seu àmbit concret".

Dani Creus, que des de la seva feina a Kaspersky Lab analitza dia a dia aquest món, assegura que "un 90% dels delictes cibernètics tenen motivacions econòmiques i es duen a terme de manera indiscriminada, buscant infeccions massives, i són oportunistes". El 10% restant, segons Creus, correspon a amenaces sofisticades que tenen com a intenció aconseguir avantatges competitius respecte als rivals, bé siguin empresarials o polítics. Hillary Clinton ha sigut una de les víctimes més famoses d'aquesta última categoria. ●