ESTILS

Lindy Hop Day a la sala Apolo, una cita per als amants del swing

Dimarts se celebra arreu del món el Lindy Hop Day, un dia dedicat als amants del swing, en què es commemora el naixement de Frankie Manning, l'ambaixador del *lindy hop* al món. Però les celebracions comencen abans i avui hi haurà una de les activitats destacades: la festa a la sala Apolo amb la Barcelona Jazz Orquestra i un convidat especial, Ricard Gili, membre fundador i director de La Locomotora Negra. La festa es fa en homenatge a Manning, i centenars d'amants del swing hi portaran les millors gales per ballar sense fre durant una bona estona.

Els virus que s'estan fent d'or gràcies als incauts

La motivació dels 'hackers' ha deixat de ser mostrar les seves habilitats i ara busquen fer-se rics

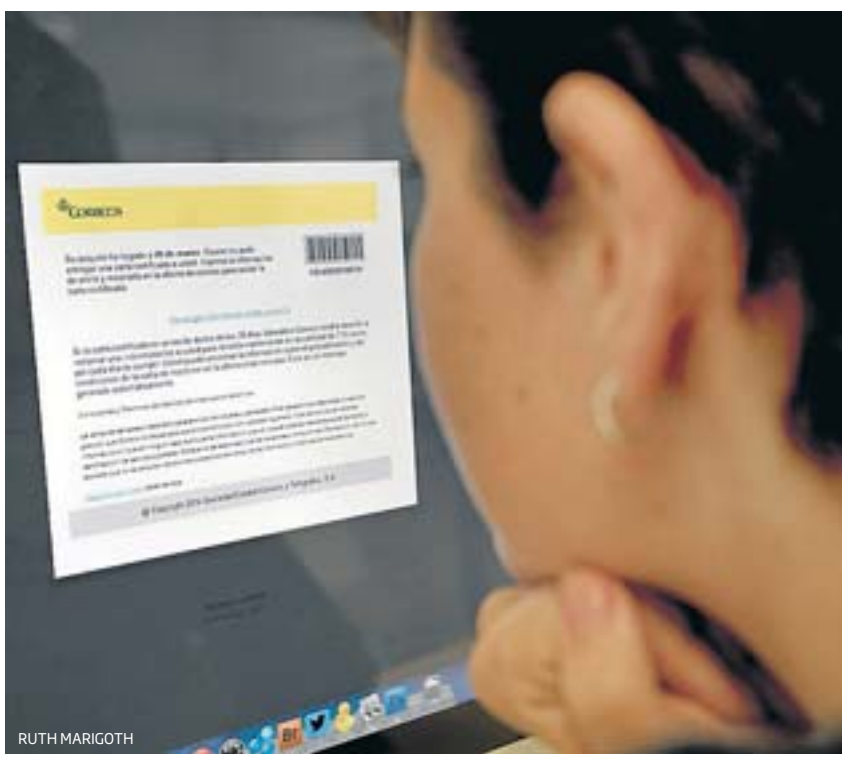
SELENA SORO
BARCELONA

L'any 1959, als laboratoris de Bell Computer, tres joves programadors –Robert Thomas Morris, Douglas McIlroy i Victor Vysotsky– van crear un joc anomenat *Core war*. El seu objectiu era que diversos programes combatessin entre ells intentant ocupar tota la memòria de la màquina i eliminar així els oponents. El que va començar com un joc va acabar convertint-se en el que molts consideren el precursor dels virus informàtics actuals.

L'any 1984 el científic Fred Cohen va encunyar per primer cop el terme *virus informàtic*, i el va definir com "el programa que pot infectar altres programes, incloent-hi una còpia possiblement evolucionada d'ell mateix". Al llarg d'aquella dècada, els *hackers* van començar a crear virus per demostrar la seva habilitat tècnica i guanyar prestigi dins els seus cercles. Durant anys aquesta ha sigut la motivació darrere la majoria de programes maliciosos. El 2005, segons Panda Security, hi va haver un canvi de tendència. "[Els *hackers*] es van adonar que l'entreteniment que suposava la creació de *malware* es podia convertir en un negoci molt rendible", diuen des de l'empresa. "Avui dia el 90% de les amenaces tenen com a motivació treure'n diners", afirma a l'ARA Dani Creus, expert de Kaspersky Lab. El 10% restant, segons diu, són atacs més dirigits a subjectes concrets, que tenen com a objectiu robar informació. En aquests casos, la motivació sol ser de caràcter polític.

En els últims anys, d'altra banda, els programes maliciosos han trobat una mina d'or en un terreny que era gairebé inexplorat: els *smartphones*, aquests petits ordinadors que ara surten de casa i acompanyen l'usuari allà on vagi. "Ara ja hi ha més mòbils que ordinadors, i per això els virus es desplacen cap a aquests dispositius: és un tema de mercat", afirma el doctor Jordi Castellà, professor al departament d'enginyeria i matemàtiques de la Universitat Rovira i Virgili. El 2013, per primera vegada, el mòbil es posicionava com l'aparell més utilitzat per accedir a internet a Espanya, per davant dels portàtils i els ordinadors de taula, segons un informe de Ditrendia. "És el mateix motiu pel qual els ciberdelinqüents sempre han atacat més els ordinadors de Windows que no els d'Apple: perquè n'hi ha més. Un 1% d'èxit d'un virus a Windows és més gran que a Mac o Linux", il·lustra l'expert en enginyeria.

CANVI DE PARADIGMA **Els experts situen en el 2005 el moment en què els *hackers* passen a fer negoci.** F. CAPUTO / GETTY



RUTH MARIGOTH

Els mòbils, finestres obertes

Jordi Castellà assenyala una altra característica dels *smartphones* que atreu l'atenció dels pirates informàtics: "El nostre Nokia de l'any 97 era una casa amb una finestra, el nostre Android d'avui dia és una casa amb milers de finestres. La informació que hi duem és molt més valuosa". Segons Josep Domingo-Ferrer, doctor expert en seguretat informàtica i professor a la URV, atacar un mòbil és molt pitjor que atacar un ordinador: "És molt més personal, controlar un mòbil és que et posin un espia a sobre que no t'abandona en cap moment".

Els telèfons mòbils, a més, són especialment vulnerables per la falta d'educació dels usuaris en temes de seguretat i també perquè és complicat instal·lar un antivirus en aquests dispositius. "No tenen prou bateria ni capacitat de càlcul, i per això els mòbils són terreny verge i adobat per als virus", assenyala Domingo-Ferrer.

Estratègia El 10% dels ciberatacs tenen com a objectiu robar informació de caràcter polític

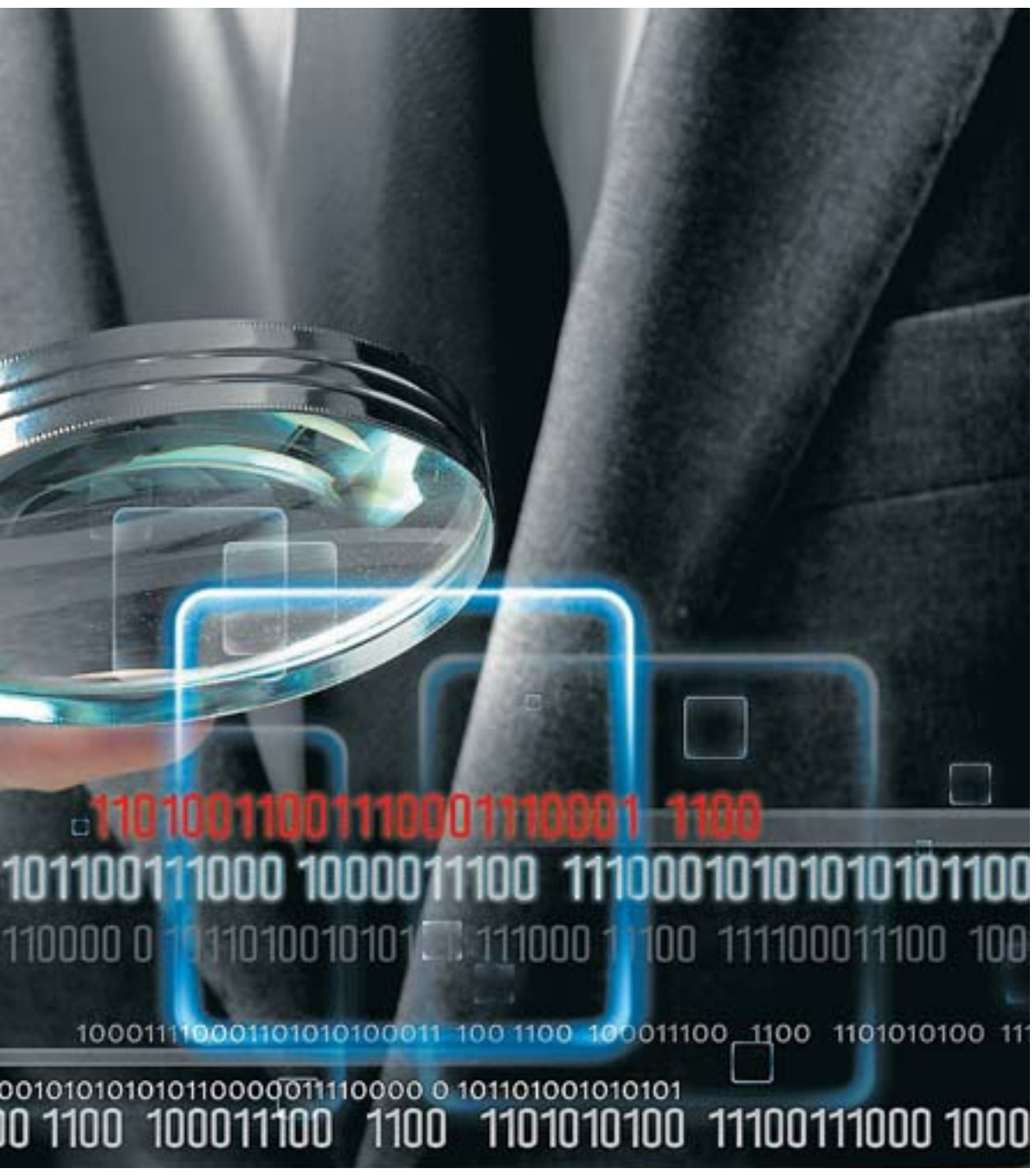
Els mètodes que pot fer servir un ciberdelinqüent per lucrar-se econòmicament gràcies al control d'un *smartphone* o un ordinador són diversos. Una de les tècniques més utilitzades és el *ransomware*, un tipus de codi maliciós que infecta l'aparell i en segresta les dades. "El *ransomware* xifra les dades i fa aparèixer un missatge a la pantalla que diu que per desxifrar-les has de fer un ingrés de 300 euros", explica Dani Creus. Últimament, el *ransomware* que més mal ha fet a casa nostra ha sigut un virus que es distribueix per correu electrònic sota l'aparença d'un missatge oficial de Correus. El missatge avisa l'usuari que li ha arribat un paquet, i adjunta un enllaç per descarregar informació sobre l'enviament. Si l'usuari hi clica, el *ransomware* segresta totes les seves dades i demana el corresponent ingrés per desbloquejar-les. Mitjançant aquest mètode, els ciberdelinqüents estan aconseguint prop de 5

La model Ariadne Artiles fa una col·lecció de bany

La model canària Ariadne Artiles ha firmat una col·lecció de banyadors per a la marca italiana Yamamay. La model s'ha inspirat en tres de les illes Canàries, Gran Canària, la Graciosa i Fuerteventura, per elaborar aquesta línia de banyadors plena de colors vius presentats amb una estètica refinada.

Tapantoni, una ruta de tapes per Sant Antoni

Fins al 31 de maig 45 establiments del barri de Sant Antoni de Barcelona oferiran una tapa amb una beguda per 2,50 euros. És la cinquena edició del Tapantoni i aquest any hi participen cinc establiments –Bar Calders, Can Cargolet, Els Ocellets, La Tata i El Dinàmic de BCN– que tindran un menú especial de 25 euros.



milions de dòlars a l'any, segons un estudi de Symantec.

De vegades els *hackers* utilitzen sistemes menys discrets i més directes per enriquir-se. Un exemple són els troians bancaris, un tipus de codi maliciós que et roba les contrasenyes quan accedeixes als teus comptes i les fa servir per transferir-se a un compte propi els teus diners. Aquest tipus de troians es poden colar per múltiples vies, com ara a través de pàgines mirall que simulen que són el portal oficial de la teva entitat bancària, però que en realitat no estan protegits mitjançant el protocol HTTPS, que garanteix que l'enviament de dades és secret i que apareix sota la forma d'un cadenat al costat de l'adreça URL. En altres ocasions, el *malware* senzillament busca aconseguir tots els teus contactes, per exemple per vendre'ls a tercers i enviar-te publicitat.

Programes gratis a internet

Una altra de les vies que estan fent servir els ciberdelinqüents per introduir *malware* als dispositius és a través d'enllaços que atrapen l'usuari amb la promesa d'alguna fotografia interessant. "Quan l'executes, el sistema s'infecta. Tu creus que només has vist la imatge però també se t'ha pogut colar un virus", explica Jordi Castellà.

L'expert en informàtica alerta també de les pàgines web que ofereixen contrasenyes per a programes de pagament, o els portals que te'ls permeten baixar directament. "Programes com l'Autocat, per exemple, valen molts diners: si algú els ha posat gratis a internet pot ser té algun interès amagat, com ara introduir un virus al teu dispositiu", conclou Castellà.

Les recomanacions dels experts per no caure en paranys

Atenció al remitent
És important no clicar enllaços ni obrir fitxers amb extensió .zip amb contrasenya i extensió .exe si en desconeixeu el contingut i, sobretot, el remitent. Segons Jordi Castellà, la conducta informàtica es pot comparar amb la sexual. "Si vas al llit amb un desconegut, has de vigilar", diu.

Pàgines sospitoses
Evitar accedir a pàgines de contingut il·legítim i procurar sempre instal·lar el programari legal del fabricant de qualsevol programa. Molts ciberdelinqüents aprofiten els arxius de pagament que es pengen en obert per introduir-hi virus informàtics.

Compte amb el mòbil
Tenir actualitzat el programari del mòbil ajudarà a controlar l'entrada de programari maliciós. Si ens connectem a alguna xarxa de wifi gratuït, és recomanable limitar-se a fer servir el mòbil per a coses que no impliquin introduir dades personals o contrasenyes. La comunicació podria no ser del tot privada o segura. Cal estar molt atents als correus electrònics estranys, ja que és el mitjà per on es transmeten més virus.