DIRECTORA
ESTHER VERA

DIRECTOR ADJUNT
IGNASI ARAGAY

DIRECTORA GERENT
GEORGINA FERRI

SUBDIRECTORS
DAVID MIRÓ
CATALINA SERRA
JORDI CORTADA

CAP DE REDACCIÓ
ENRIC BORRÀS

DIRECTORA D'ART
CRISTINA CÓRDOBA

EDICIÓ PAPER
ROSA RODON
POLÍTICA
GERARD PRUNA
INTERNACIONAL
FRANCESC MILLAN
SOCIETAT
ELENA FREIXA
ECONOMIA
ALBERT MARTÍN
DEBAT
TONI GÜELL
CULTURA
LAURA SERRA
ESTILS
THAIS GUTIÉRREZ
MÈDIA
ÀLEX GUTIÉRREZ
ESPORTS
XAVI HERNÁNDEZ NAVARRO
DELEGADA MADRID
MARIONA FERRER
LLENGUA
MARIA RODRÍGUEZ
FOTOGRAFIA
XAVIER BERTRAL
DISSENY DIGITAL
RICARD MARFÀ
ARA TV
ALBA OM

EDICIÓ DE PREMSA PERIÒDICA ARA, SL

PRESIDENT
FERRAN RODÉS
FINANCES
XAVIER LINARES
MÀRQUETING I VENDES
PABLO CASALS
COMERCIAL
SERGI GERMÁN
NOUS NEGOCIS
ORIOL CANALS
TECNOLOGIA
MARC CAMPRODON

DIRECTOR FUNDADOR
CARLES CAPDEVILA

C/ DIPUTACIÓ, 119
08015 BARCELONA.
TELÈFON: 93 202 95 95.
ATENCIÓ AL SUBSCRIPTOR:
93 275 11 10
subscripcions@ara.cat

DL.: B-42598-2010
ISSN: 2014-010X

EL DIARI D'AHIR

Fe d'errades: L'ARA agraeix als lectors que ens facin arribar els errors que detectin en el contingut dels articles. Un cop confirmat l'error, l'ARA publica la fe d'errades en aquesta mateixa columna. Podeu fer-nos arribar les vostres esmenes a opinio@ara.cat.

DEBAT

CONSULTEU MÉS ARTICLES A L'ARA.CAT

Què són els atacs de 'ransomware'?

JOSEP DOMINGO FERRER

CATEDRÀTIC D'ENGINYERIA INFORMÀTICA DE LA URV I DIRECTOR DEL CYBERCAT

Aquests dies ha estat tristament notícia l'atac informàtic patit per la Universitat Autònoma de Barcelona que ha inutilitzat tota la seva infraestructura informàtica. En el moment d'escriure aquestes línies, els serveis d'informàtica de la universitat treballen intensament per anar netejant de programari maliciós zones de la xarxa informàtica amb vista a poder-les posar de nou en funcionament. Encara no ha transcendit la naturalesa exacta de l'atac ni els danys que ha ocasionat, tot i que sembla que hi ha tingut algun paper el programari maliciós de rescat, en anglès *ransomware*. Caldrà esperar que la situació es resolgui per saber com ha anat, però no és sobrer que els ciutadans coneguin més aquesta mena d'atacs.

El programari maliciós de rescat és un programari d'extorsió que pot blocar un ordinador i demanar un rescat per desblocar-lo. Els rescats se solen demanar en criptomoneda, normalment bitcoins, per tal que sigui més difícil de rastrejar on va el pagament. Un ordinador es pot infectar de diverses maneres, per exemple quan el seu usuari visita un lloc web maliciós, descarrega un fitxer maliciós annexat a un correu electrònic o bé instal·la sense voler un complement maliciós (*add-on*) en fer una descàrrega d'altres fitxers o programes. El programari maliciós està dissenyat per esquivar la detecció tant de temps com sigui possible i quedar latent. Es recomana fer servir programari de defensa (antivirus i altres) per intentar detectar i eliminar *ransomware*. De tota manera, alguns símptomes que ens han de fer sospitar que patim una infecció són canvis en les extensions de fitxers o una activitat injustificadament alta de la unitat de control (CPU) del nostre ordinador.

Els grans atacs basats en *ransomware* no solen ser purament automàtics, sinó que combinen la propagació automàtica de programari maliciós amb actuacions manuals dels pirates, encaminades a arribar a equips amb accessos més privilegiats a partir dels equips inicialment atacats pel programari. Els pirates poden robar les dades i les contrasenyes que trobin als ordinadors que envaeixen. En aquest sentit, convé no guardar grans quantitats de dades al nostre ordinador, ni apuntar usuaris i contrasenyes en cap fitxer i ni tan sols guardar-les al navegador.

En aquest moment els atacs de programari maliciós de rescat són una plaga a tot el món. S'estima que enguany (2021) se'n produeix un cada 11 segons i que el perjudici econòmic global a final d'any pujarà a 20.000 milions de dòlars. Per comparació, el 2019 només hi havia un atac cada 14 segons. El sector públic és un dels objectius preferents de les màfies del *ransomware*, en particular els ajuntaments (recordem el cas de l'Ajuntament de Cambrils aquest Nadal). Les raons cal cercar-les en la gran quantitat de dades que acumulen els organismes públics (i que els pirates cobegen), així com en el fet que solen tenir menys pressupost de ciberseguretat i més obertura que organitzacions privades de mida comparable.

GETTY

Els atacs informàtics com el que ha patit la UAB són una plaga a tot el món. S'estima que enguany se'n produeix un cada 11 segons

Val a dir, però, que és probable que el sector privat pateixi més atacs de *ransomware* dels que s'arriben a saber. En una empresa, la pressió per pagar rescats per recuperar dades crítiques i evitar danys reputacionals pot ser molt alta. D'altra banda, als EUA el govern ha alertat que les infraestructures crítiques del país estan també patint cada cop més atacs d'aquesta mena.

Què podem fer per prevenir un atac de programari maliciós? En primer lloc, seguir les instruccions dels serveis informàtics de la nostra organització. En ordinadors domèstics, hem de mantenir actualitzat el sistema operatiu i totes les aplicacions, instal·lar-hi un bon programari antivirus i fer periòdicament còpies de seguretat dels nostres arxius. A part, hem d'evitar activitats de risc, com visitar pàgines web sospitoses, descarregar contingut dubtós o obrir fitxers annexos rebuts de remitents desconeguts.

Què fer un cop hem estat atacats i tenim l'ordinador blocat? Primer de tot, si és un ordinador de la nostra empresa o de la nostra universitat, cal informar-ne els responsables informàtics. Si la decisió del que cal fer és nostra, caldria provar-ho tot abans de pagar el rescat, per no engreixar les màfies. Es pot intentar netejar l'ordinador amb l'ajut de programari de defensa i d'especialistes. Si no ens en sortim, caldrà reinicialitzar-lo amb les opcions de fàbrica i mirar de restaurar posteriorment una còpia de seguretat anterior que sapiguem que és neta.

Malauradament, els atacs per programari maliciós de rescat ens continuaran afectant fins que les organitzacions deixin d'infectar-se i de pagar els rescats. Mentrestant, convé que les agències de ciberseguretat rebin tota la informació possible sobre els atacs que es produeixen. Per vèncer un enemic és fonamental conèixer-lo bé.