SEGURETAT DIGITAL

Les grans empreses compren escuts per als atacs de la web profunda

S'hi amaguen els delinqüents digitals, però també activistes perseguits

NEREIDA CARRILLO
BARCELONA

Les empreses es protegeixen cada vegada més contra els atacs. GETTY

Els negocis d'aquest segle tenen bona part de la seva activitat a internet. Protegir-se d'atacs informàtics, del robatori d'informació o d'altres malifetes digitals esdevé una necessitat que cal satisfer amb mètodes cada cop més sofisticats. Ara el centre tecnològic Eurecat ofereix a les empreses forjar-se un escut contra bona part d'aquests atacs, els que es couen a la *deep web* o web profunda. El servei, anomenat Deepsec, permet rastrejar la web profunda per detectar el que pugui comprometre la seguretat de les companyies.

El director de la unitat d'IT Security d'Eurecat, Gonzalo Asensio, explica que a les empreses els interessa saber si en aquest espai s'estan preparant atacs per fer caure les seves webs, si es comercia amb usuaris i contrasenyes per accedir a informació privilegiada, si circulen missatges amb noms dels seus directius o si venen números de targetes bancàries i codis per operar i robar diners. La web profunda inclou les pàgines no indexades als cercadors, un conjunt enorme i heterogeni que comprèn des d'intranets o comunicacions d'activistes perseguits per les seves idees fins a activitats delictives. Els malfactors s'aprofiten que les comunicacions són anònimes i xifrades.

Detectar atacs

El costat més perillós de la web profunda s'anomena web fosca o *dark net*. És aquí on s'accentua l'activitat delictiva i on, segons Asensio, tenen més credibilitat les credencials que es bescanvien en un mercat negre, en què es comercia habitualment amb *bitcoins*. "La informació que s'obté a la *deep web* serveix per prendre mesures proactives de seguretat", afirma Asensio. Descobrir a la web profunda una vulnerabilitat de la web pot permetre reparar-la abans dels atacs i detectar números de targetes robades facilita el bloqueig abans que els lladres les utilitzin.

Asensio explica que la majoria de clients de Deepsec són bancs i asseguradores, però també percep interès d'altres sectors com la sanitat. El servei, actiu des de fa un any, continua Asensio, "és similar al del Google Alerts", amb la diferència que, com que la informació de la web profunda no s'indexa ni es localitza fàcilment, la cerca es fa amb tècniques complexes. Les empreses, però, poden configurar cerques per paraules o xifres per fer indagacions a la web profunda.

Amagatall per als lladres

Tot plegat permet a les empreses actuar abans que es cometi el delicte i sense haver de recórrer a la policia. Els diversos experts consultats per l'ARA asseguren que els mecanismes de la web profunda, on les comunicacions són gairebé del tot anònimes, dificulten la feina dels cossos de seguretat. "El xifrat comporta més problemes. No és el mateix que la gent enviï postals que cartes tancades", afirma Jordi Iparraguirre, enginyer informàtic i membre del capítol català de la Internet Society.

Entre els problemes de seguretat informàtica que poden patir les empreses, no tots relacionats amb la web profunda, els experts destaquen el segrest de les dades, la fuga d'informació o el *phishing*. L'impulsor del congrés No cON Name i expert en seguretat informàtica José Nicolás Castellano explica que el primer és un atac que "aprofita una vulnerabilitat al sistema, xifra i segresta les dades i exigeix un pagament". La fuga d'informació, explica Iparraguirre, es pot produir per una acció "des de fora o des de dins", en què s'accedeix a informació privilegiada. El *phishing* comporta accedir a dades confidencials a través, per exemple, d'un correu electrònic que aparentment prové d'una font fiable i en el qual s'inclou un enllaç per consumar el frau.