

L'Agència de Ciberseguretat de Catalunya alerta d'una triple amenaça de programaris maliciosos

written by Redacció Unilateral | 12 de febrer de 2020

Els programaris maliciosos s'han convertit en una eina d'ús recurrent pels cibercriminals que tenen com a objectiu prioritari les empreses, tot i que durant el tercer trimestre del 2019 també han destacat els atacs contra organismes públics i en especial el sector educatiu, coincidint amb l'inici del curs escolar. La motivació econòmica és cabdal per entendre l'evolució, complexitat i polivalència d'aquests ciberatacs.

L'última edició de [l'Informe de tendències de ciberseguretat de l'Agència de Ciberseguretat de Catalunya](#), que fa un extens repàs a les principals ciberamenaces detectades al món i té en compte fonts qualificades d'entitats, fabricants, organismes i professionals de l'àmbit de la ciberseguretat, alerta de la triple amenaça distribuïda arreu del món a través de correus electrònics amb un fitxer adjunt maliciós.

D'acord amb aquest informe, aquests atacs amaguen l'autoria combinada de diversos operadors criminals que fan ús de tres programaris maliciosos diferents: els troians *Emotet* i *Trickbot* que forcen els dispositius infectats a quedar sota el control d'una xarxa d'ordinadors (*botnet*) controlada des d'un servidor, i el programari de segrest *Ryuk*, encarregat de xifrar els sistemes d'informació de la víctima.

Qualsevol dispositiu connectat a Internet és susceptible de formar part d'una *botnet* i s'estima que en alguns casos han arribat a tenir una mida d'uns dos milions i mig de

dispositius. Per aquest motiu són tan importants les mesures preventives, com la conscienciació dels treballadors contra un atac d'enginyeria social (*phishing*) i l'ús de sistemes ben protegits, actualitzats i monitoritzats.

Afectació a Catalunya

Els virus informàtics de segrest de dades (*ransomware*) són un dels principals perills per a les empreses que cada cop més són requerides a pagar rescats elevats per recuperar els fitxers segrestats.

La campanya de *ransomware* de la triple amenaça ha arribat a Catalunya on múltiples incidents han tingut ressò mediàtic. Els consistoris de Tremp, Esterri d'Àneu i Seròs en van ser víctimes i la Diputació de Lleida va aturar l'atac a temps en ser alertada. L'Ajuntament de Lloret de Mar va patir la inhabilitació de molts dels seus serveis durant més de dues setmanes i el Laboratori de Referència de Catalunya (LRC), així com els sis centres assistencials amb qui treballar habitualment, també en van resultar afectats. Diverses empreses privades de Lleida i Girona també van ser objecte d'atacs.

Dia de la Internet Segura

Més enllà de l'amenaça del programari de segrest (*ransomware*), l'informe destaca que el rastre que deixen les persones a Internet permet als cibercriminals obtenir dades per usurpar la identitat digital i cometre tot tipus de frau. En aquest sentit les bones pràctiques dels usuaris són fonamentals.

Amb motiu de la celebració ahir del Dia de la Internet Segura que es celebra arreu del món, des de l'Agència de Ciberseguretat de Catalunya es recorda la necessitat de mantenir uns hàbits cibersaludables en el nostre dia a dia digital.

Des del programa de Govern **Internet Segura** s'han preparat una

sèrie d'activitats adreçades al món escolar, les famílies i la ciutadania en general. A través de diverses propostes, com ara jocs i tallers, entre d'altres, i l'anàlisi dels drets digitals es proposa treballar el civisme i la ciberseguretat a Internet.

Més informació a InternetSegura.cat