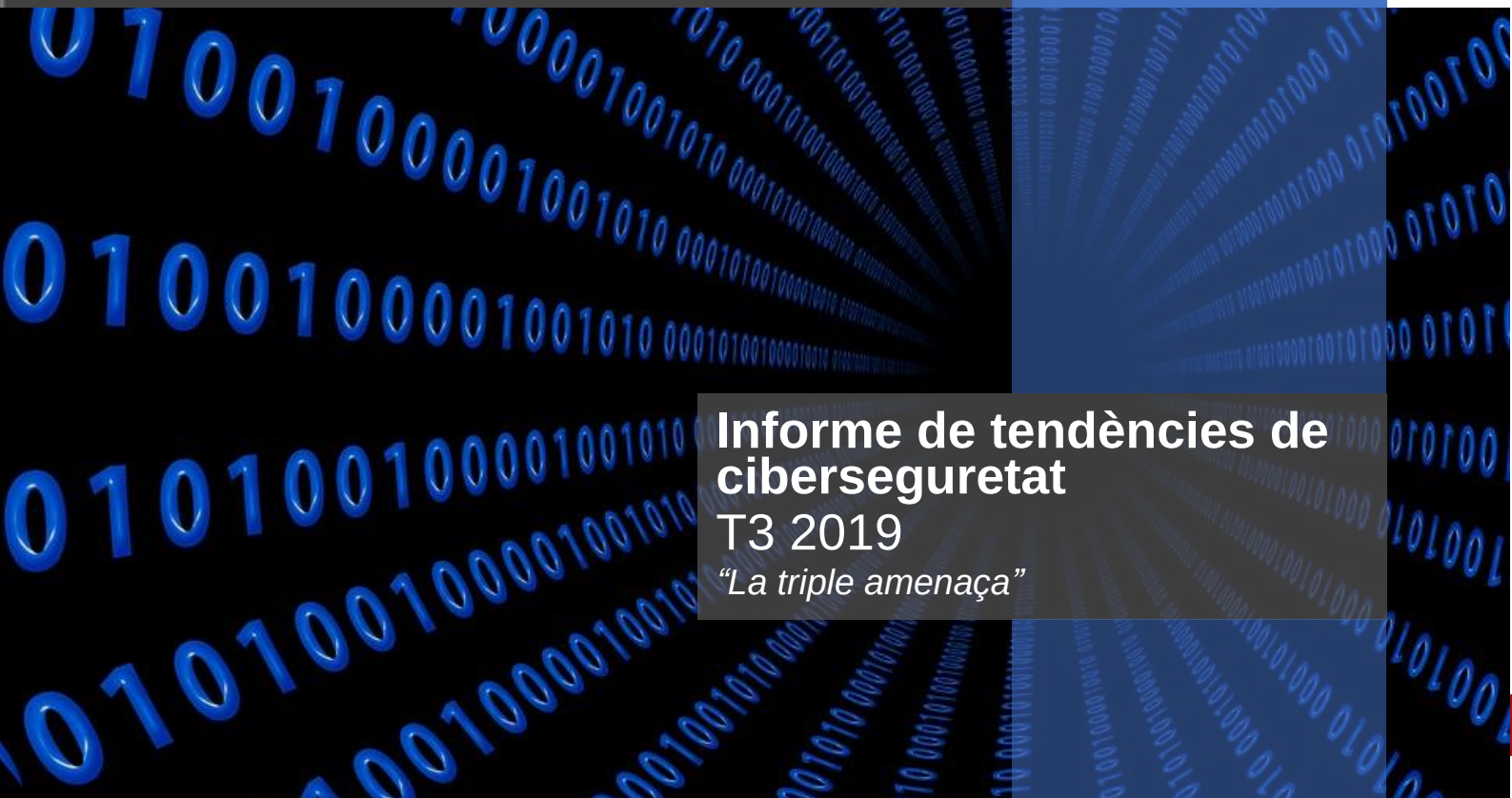
Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

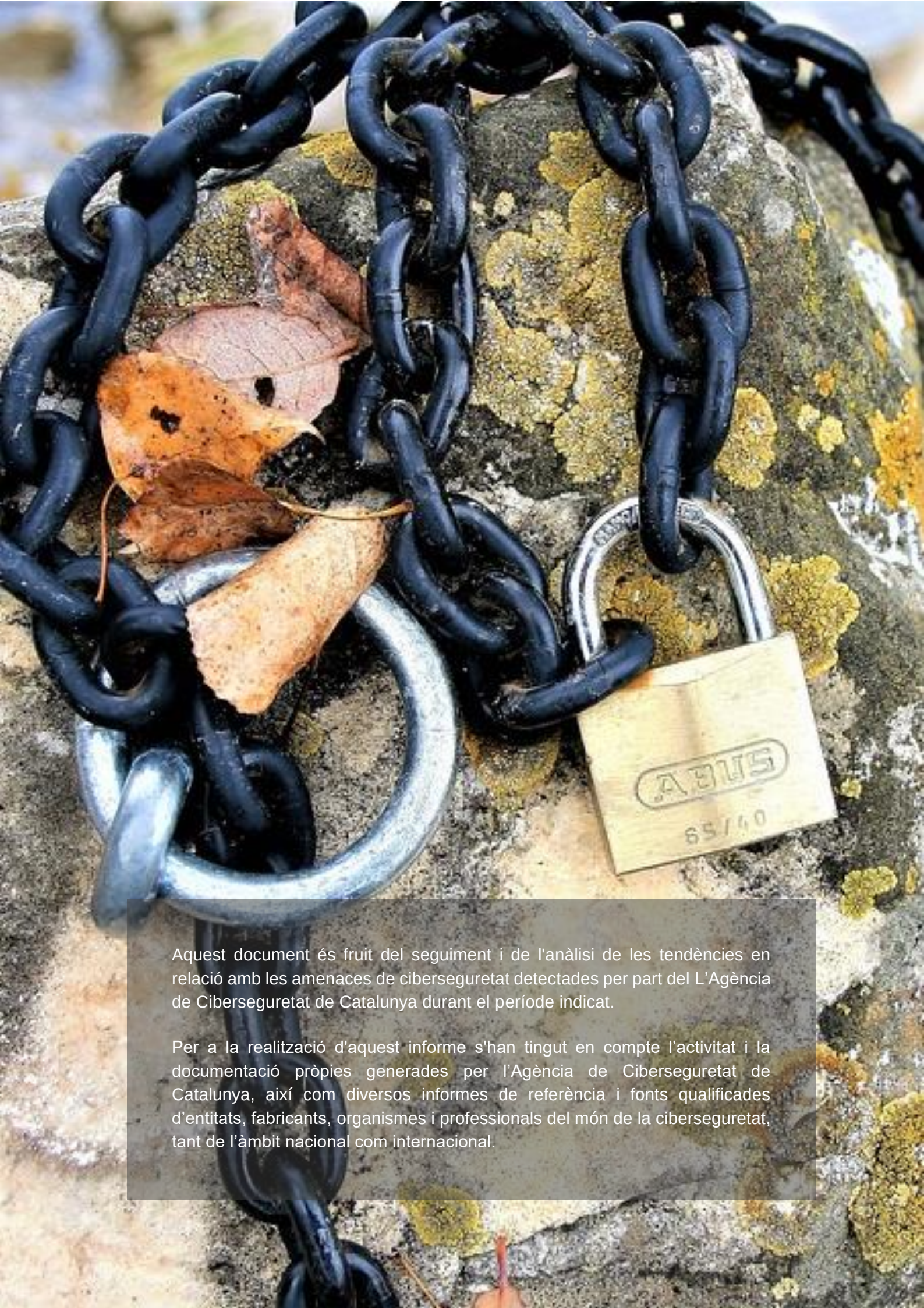


Informe de tendències de ciberseguretat

T3 2019

"La triple amenaça"

Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya



Aquest document és fruit del seguiment i de l'anàlisi de les tendències en relació amb les amenaces de ciberseguretat detectades per part del L'Agència de Ciberseguretat de Catalunya durant el període indicat.

Per a la realització d'aquest informe s'han tingut en compte l'activitat i la documentació pròpies generades per l'Agència de Ciberseguretat de Catalunya, així com diversos informes de referència i fonts qualificades d'entitats, fabricants, organismes i professionals del món de la ciberseguretat, tant de l'àmbit nacional com internacional.

Índex

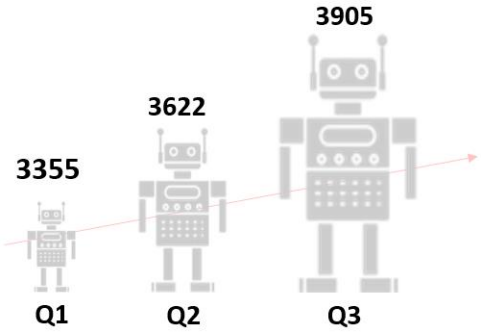
Resum

Resum

L'agenda de la ciberseguretat del 3r trimestre de 2019 ha vingut marcada per l'ús de *botnets* per a la difusió de *ransomware* i, d'altra banda, els múltiples casos d'usurpació d'identitat.

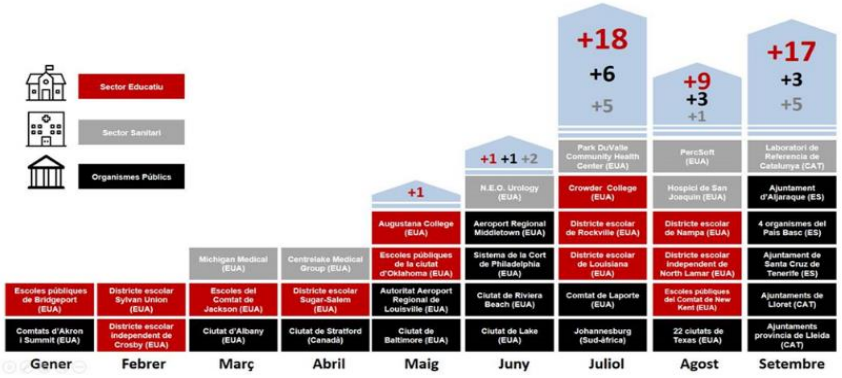
Botnets. Les *botnets* proliferen molt ràpidament, com ho fan els dispositius amb connectivitat a Internet. **Estan formades per tot tipus de dispositius i qualsevol dispositiu connectat a Internet és susceptible de formar-ne part**. Són utilitzades **per portar a terme diferents tipus d'accions malicioses** com atacs DDoS, enviament de correu brossa o *phishing,* atacs de força bruta o execució de *malware*, entre d'altres. Ha estat qüestió de temps que el cibercrim aconseguís utilitzar-les per **dirigir la difusió de *ransomware* i possibilitar campanyes d'abast global**. En aquesta línia, destaquen les *botnets* **Emotet** i **Trickbot**, protagonistes d'una important campanya d'atacs de *ransomware* d'abast mundial amb impacte en **organismes catalans i espanyols.**

NOUS SERVIDORS DE BOTNETS PER TRIMESTRE

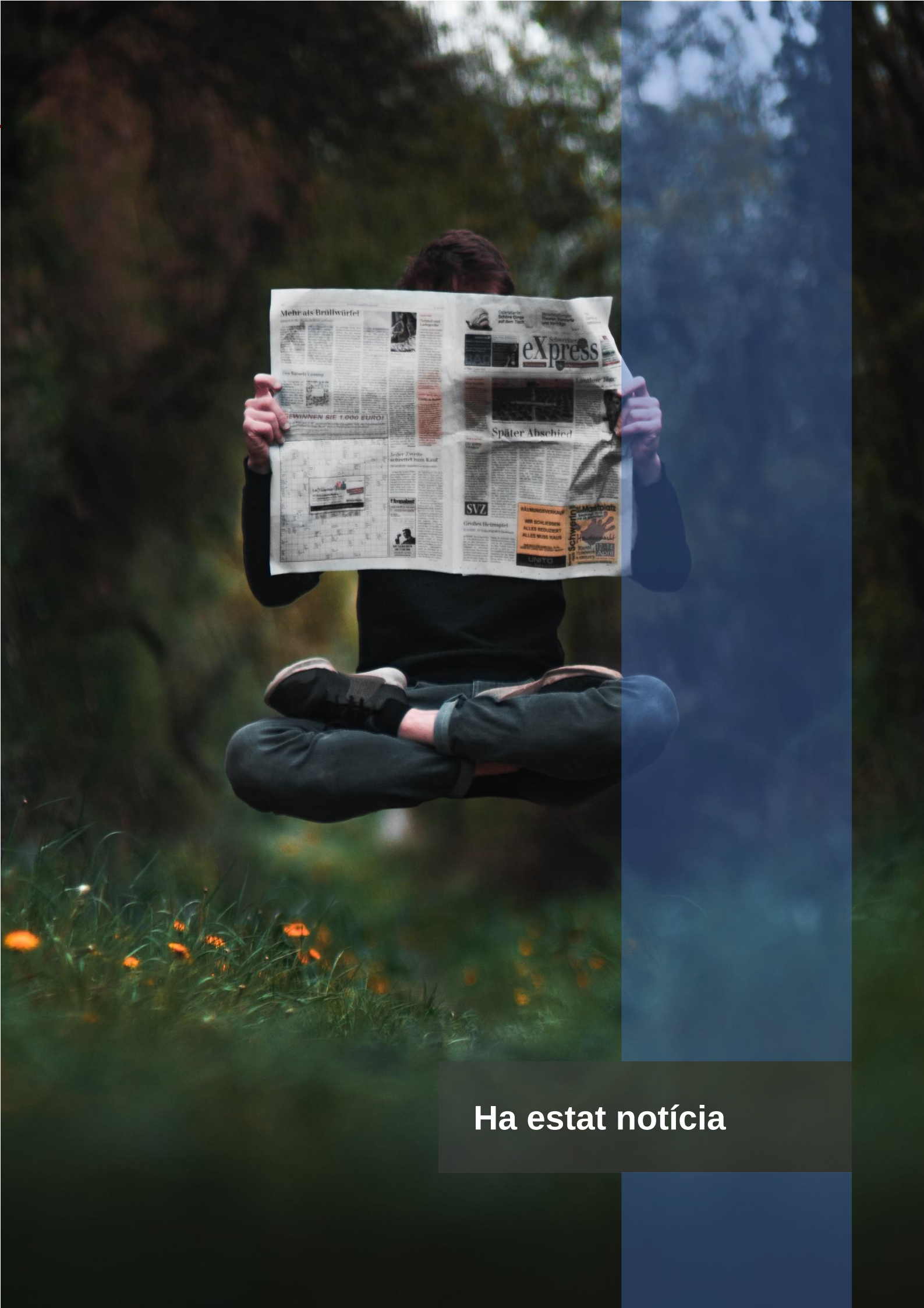


Ransomware* dirigit.** Aquest tercer trimestre de 2019 ha destacat per **l'increment dels atacs dirigits amb *ransomware. L'atac a través de les connexions d'escriptori remot (RDP) ha esdevingut el vector d'atac favorit dels ciberdelinqüents per accedir als sistemes d'informació de les víctimes i infectar-les amb *ransomware*. Les organitzacions són l'objectiu prioritari, especialment les empreses, tot i que aquest trimestre destaquen els atacs contra el **sector públic i, en especial, el sector educatiu,** coincidint amb l'inici del curs escolar. **L'imperatiu dels centres educatius per estar operatius en època d'inscripcions**, juntament amb la falta de recursos dedicats a la ciberseguretat, els **ha dut a ser un objectiu preferent per als atacants**. El màxim exponent d'aquest fet es va produir aquest setembre, quan un *ransomware* va infectar el districte escolar de Monroe (**Nova York**) i va afectar **un total de 49 escoles el dia abans de l'inici del curs**, fet que va provocar que aquest s'endarrerís uns dies.

PRINCIPALS INCIDENTS PER RANSOMWARE DETECTATS AL SECTOR PÚBLIC



Usurpació d'identitat. El **rastre que deixen les persones a Internet** permet als cibercriminals obtenir el perfil de les seves víctimes per usurpar la identitat digital amb l'objectiu d'obtenir algun tipus de benefici, principalment econòmic. Obtenir les dades que permetin la suplantació o el robatori d'identitat **és el gran objectiu dels ciberatacants** i, per aquest motiu, ataquen els servidors on les dades estan emmagatzemades, fan ús de tècniques de *phishing*, o bé les compren a la *dark web* quan han estat obtingudes per un tercer. Amb les dades adequades, un ciberatacant podrà **segrestar un compte de xarxes socials o suplantar identitats per cometre tot tipus de fraus**, com ara la creació fraudulenta de comptes bancaris, aprofitar-se de la identitat mèdica o fer un ús fraudulent d'una targeta de crèdit. L'ús de mesures de ciberseguretat, com el xifrat de la informació, les bones pràctiques dels usuaris, les regulacions legals i els nous **models de gestió d'identitats, com la identitat sobirana**, són prometedors de cara a mitigar aquesta problemàtica.



Ha estat notícia

Ha estat notícia

Un troià és un programa maliciós amb una funció aparentment útil, però amb funcions addicionals amagades que faciliten l'accés no autoritzat a un sistema i el fan vulnerable.

Com el cavall de Troia, sota una aparença benèvola s'hi amaga una amenaça.

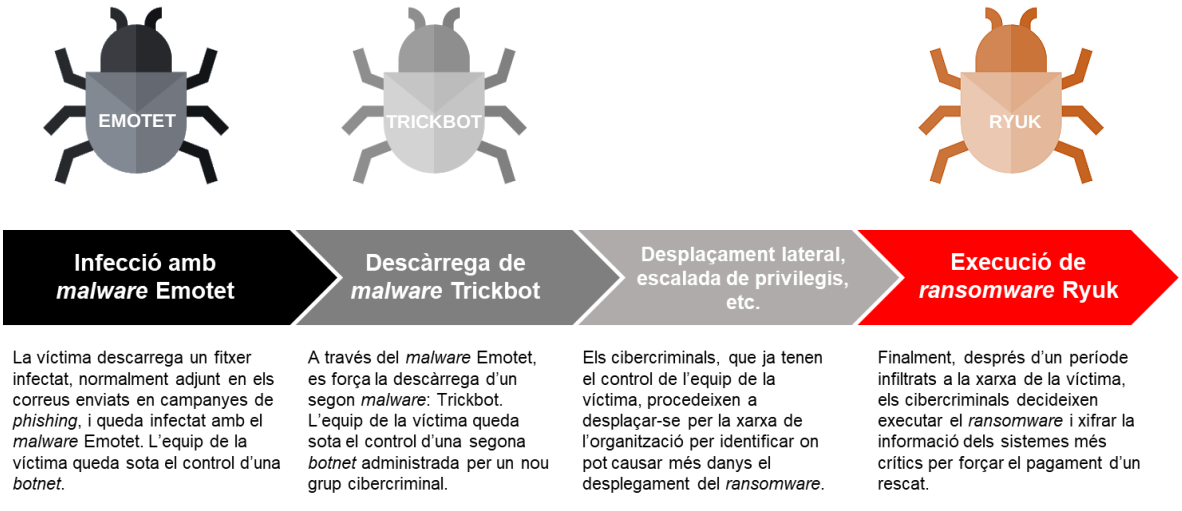
Un dropper es un malware que ha estat dissenyat per instal·lar programari maliciós a un sistema d'informació.

Campanya de *ransomware* global

En els anteriors informes trimestrals de l'any 2019 s'ha identificat un augment dels atacs dirigits de *ransomware* arreu del món[1] contra empreses i organismes públics. La companyia **Norsk Hydro**[2] i la ciutat de **Baltimore**[3], les quals han patit llargs períodes d'inactivitat i enormes costos, **han estat casos exemplificants de les greus conseqüències que un atac de *ransomware* pot comportar**.

La companyia Norsk Hydro i la ciutat de Baltimore (...) han estat casos exemplificants de les greus conseqüències que un atac de ransomware *pot comportar.*

Aquest trimestre ha destacat per la campanya de *ransomware* d'abast mundial amb la forma de **triple amenaça**, atès que fa ús de **tres programaris maliciosos diferents**: el troià **Emotet** i el també troià **Trickbot**, que forcen els dispositius infectats a formar part d'una ***botnet*** (veure detall del funcionament al capítol *Botnets*), i el *ransomware* **Ryuk**, encarregat de xifrar la informació de la víctima (veure capítol *Ransomware* dirigit)**.** Aquesta campanya **ha estat distribuïda arreu del món** a través de correus electrònics que contenien un arxiu Word amb codi maliciós i ha aprofitat el potencial com a *dropper* de les *botnets* per a la descàrrega de nou *malware*. Un dels principals focus d'afectació han estat els Estats Units (EUA) on, des de l'atac el juny passat a l'Ajuntament de Lake City, a Florida, s'han incrementat notablement el nombre d'incidents.



Il·lustració 1. Fases de l'atac en la campanya de difusió del ransomware *Ryuk*

[1] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/Informe-de-Tendencies-1er-trimestre-2019*
[2] *https://www.thethreatreport.com/norsk-hydros-damage-control-efforts-after-ransomware-attack/*
[3] *https://www.govtech.com/security/Estimates-Put-Baltimores-Ransomware-Recovery-at-18-2-M.html*

A **Austràlia**, l'ACSC (Australian Cyber Security Centre) va confirmar un total de **19 infeccions** sospitoses d'**infraestructures crítiques, hospitals i agències governamentals** afectades per la triple amenaça[4]. Països com **Itàlia**[5], **Alemanya**, **Polònia**, **Anglaterra**[6], **Hong Kong** o **Singapur**[7], entre d'altres, han tingut incidents similars.

Afectació a Catalunya

La campanya de la triple amenaça ha arribat a Catalunya on múltiples incidents s'han publicat als mitjans a causa del seu impacte. No obstant això, segur que **són molts més els que no han tingut ressò mediàtic**.


Diari de Girona
Un virus informàtic afecta el laboratori que treballa per a sis hospitals catalans
Només atendrà analítiques urgents a través d'un circuit alternatiu que protegeix les dades

Il·lustració 2. Titular publicat al Diari de Girona[8]

Els **consistoris de Tremp, Esterri d'Àneu i Seròs van ser víctimes** de la triple amenaça[9] i la **Diputació de Lleida va poder aturar l'atac** a temps en estar alertada. L'**Ajuntament de Lloret va patir la inhabilitació de molts dels seus serveis** durant més de dues setmanes**,** fet que va provocar que el consistori ampliés els terminis per a la realització dels tràmits com a mesura pal·liativa[10]. El **Laboratori de Referència de Catalunya (LRC)**, així com els sis centres assistencials amb qui treballa habitualment, van resultar afectats fins al punt que **van veure's obligats a atendre les peticions més urgents a través de circuits alternatius i col·laboracions amb altres laboratoris**. També, es va detectar la presència del *malware* **Emotet**, utilitzat en la primera fase de l'atac contra diverses **empreses privades de Lleida[11] i Girona**, tot i que no s'ha fet pública l'afectació.

Afectació a la restat de l'Estat

La campanya de *ransomware* global també ha tingut una forta propagació pel territori espanyol, on s'han detectat casos al País Basc, Andalusia i les Illes Canàries.


deia
Un ataque masivo de correos con virus afecta a diversos entes públicos vascos
La Ertzaintza investiga cuatro denuncias y el Centro Vasco de Ciberseguridad coordina la respuesta con las instituciones

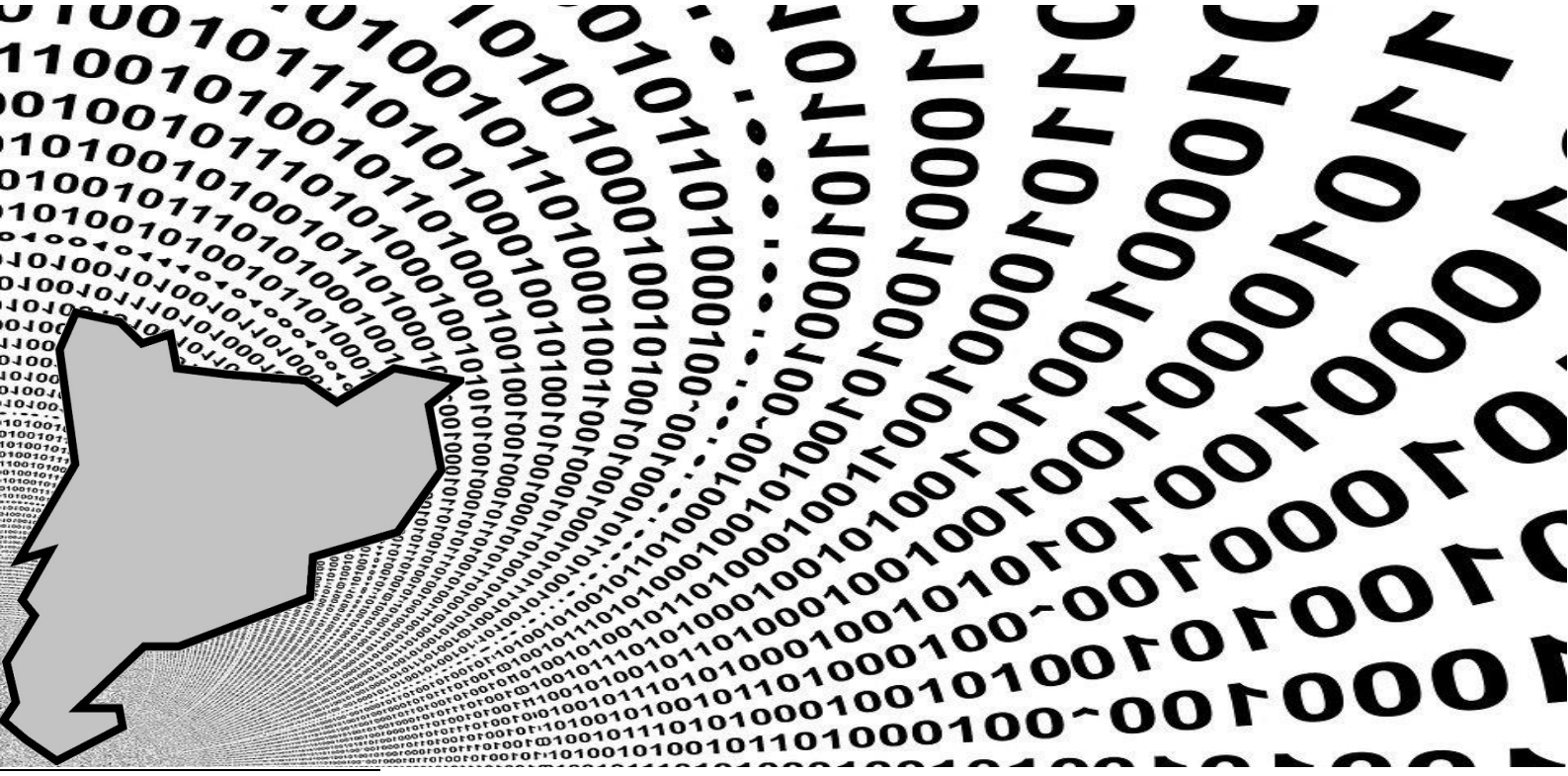
Il·lustració 3. Titular publicat al Diari Deia

[4] *https://www.computerworld.com/article/3471081/critical-infrastructure-providers-government-agencies-hit-by-emotet.html*
[5] *https://tecnologia.libero.it/italia-sotto-attacco-informatico-il-rischio-emotet-e-come-difendersi-30822*
[6] *https://www.2-spyware.com/after-months-of-silence-emotet-came-back-with-a-new-malspam-campaign*
[7] *https://www.helpnetsecurity.com/2019/11/11/emotet-returns/*
[8] *https://www.diaridegirona.cat/catalunya/2019/10/02/virus-informatic-afecta-laboratori-que/1005606.html*
[9] *https://www.segre.com/noticies/comarques/2019/09/25/suplanten_mails_ajuntaments_lleida_per_propagar_virus_informatics_87532_1091.html*
[10] *https://www.elpuntavui.cat/societat/article/5-societat/1675575-un-atac-informatic-bloqueja-els-ordinadors-de-l-ajuntament-de-lloret.html*
[11] *https://www.segre.com/noticies/comarques/2019/09/26/el_virus_informatic_dels_ajuntaments_arriba_la_diputacio_empreses_privades_87614_1091.html*

Al País Basc, l'**Ertzaintza i el Centro Vasco de Ciberseguridad** han actuat per la denúncia d'almenys quatre entitats. **L'Ajuntament de Santurtzi ha estat un dels més afectats**, ja que va comprometre els ordinadors dels funcionaris i el servidor que gestiona tot el consistori, paralitzant diverses àrees de l'ajuntament. La **fundació Hazi**, dedicada a impulsar la competitivitat i sostenibilitat del sector primari, també en va resultar atacada, així com la **Diputació de Bizkaia**, la qual va reconèixer l'afectació en **la relació telemàtica amb els biscaïns.** L'**Ajuntament de Bilbao** també va reconèixer ser objecte de l'atac, però van aconseguir parar-lo a temps[12].

A Andalusia, els **ajuntaments de Jerez**[13] i **Aljaraque**[14] també en van ser víctima. **A Jerez es van desconnectar els 50 servidors de la seva xarxa interna per a evitar que l'atac es propagués** i pogués infectar expedients, denúncies de la policia o el sistema de pagament de taxes. Segons declaracions de l'alcaldessa, tan sols va resultar compromesa la informació dels correus electrònics d'ordinadors infectats. Per la seva part, l'agrupació de tècnics municipals va ressaltar la manca de renovació de la infraestructura informàtica de l'ajuntament i la precarietat del suport informàtic.

Més enllà del País Basc i Andalusia, s'ha donat a conèixer com l'**Ajuntament de Santa Cruz de Tenerife** també va resultar impactat per la campanya de *ransomware*, tot i que cal destacar que el seu departament de noves tecnologies **va actuar amb rapidesa** i van tenir un impacte mínim sobre els serveis municipals[15].



[12] *https://www.deia.eus/2019/10/01/sociedad/euskadi/un-ataque-masivo-de-correos-con-virus-afecta-a-diversos-entes-publicos-vascos*
[13] *https://www.xataka.com/seguridad/paralizan-ayuntamiento-jerez-encriptando-su-base-datos-virus-informatico-piden-rescate-para-liberarlo*
[14] *https://www.europapress.es/andalucia/huelva-00354/noticia-ayuntamiento-aljaraque-huelva-denuncia-ataque-virus-informatico-20191002184916.html*
[15] *https://www.eldia.es/santa-cruz-de-tenerife/2019/09/26/consistorio-sufre-ataque-informatico-afecta/1011582.html*

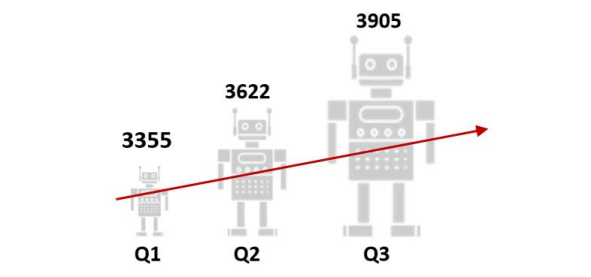

Botnets

Baròmetre

Mirai, Satori, les darrerament omnipresents, Emotet, Trickbot, Dridex... Totes són *botnets* conformades per dispositius que controla un cibercriminal des d'un servidor C&C (*Command and Control*). Totes elles muten i, dia a dia, creixen en funcionalitats i capacitat de propagació.

Proliferació de *botnets*

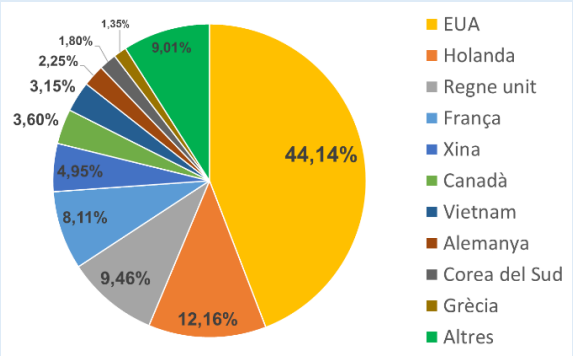
Les *botnets* proliferen com ho fan els dispositius amb connectivitat a Internet i han esdevingut un autèntic risc pel desenvolupament de la pròpia xarxa. El darrer any han estat en constant creixement, especialment aquest tercer trimestre.



Il·lustració 4. Servidors pel control de botnets *detectats el 2019*[16]

Geografia de les *botnets*

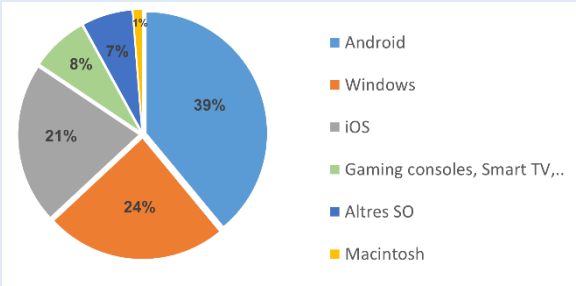
Només 10 països concentren més del 90% dels servidors de control de les *botnets* conegudes i Europa ja en concentra un terç del total.



Il·lustració 5. Distribució dels servidors de control de botnets *per països*[17]

Atacs DDoS

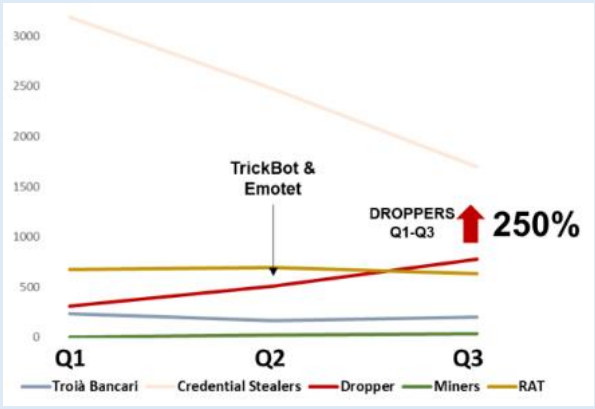
Les *botnets* estan formades per tot tipus de dispositius i qualsevol dispositiu connectat a Internet és susceptible de formar-ne part. A partir de l'anàlisi dels atacs DDoS, sorprèn constatar com un 50% d'aquests atacs prové de dispositius Android i iOS.



Il·lustració 6. Dispositius origen dels atacs DDoS[18]

Tipologies de *botnet*

Destaca el creixement de la difusió de *botnets* amb funcionalitats de *dropper*, especialitzades en la descàrrega d'altres tipus de *malware.* El ressorgiment de *botnets* com Emotet i Trickbot, n'és la causa principal, atès que s'utilitzen per a la difusió de *ransomware*, una activitat especialment lucrativa i interessant pel cibercrim.



Il·lustració 7. Deteccions de tipus de programari maliciós difós per botnet[19]

[16] *https://www.spamhaus.org/news/article/789/spamhaus-botnet-threat-update-q3-2019*
[17] *https://securelist.com/ddos-report-q2-2019/91934/*
[18] *https://www.nexusguard.com/threat-report-q1-2019*
[19] *https://www.spamhaus.org/news/article/789/spamhaus-botnet-threat-update-q3-2019*

Botnets

Una botnet és grup d'ordinadors zombi que són controlats des d'un mateix servidor i es fan actuar conjuntament.

El terme prové de l'acrònim en anglès de les paraules robot (bot) i net (xarxa), on cada dispositiu que forma part de la mateixa és anomenat bot o zombi.

Un servidor de comandament i control (C&C) és un ordinador central que emet ordres a una xarxa de zombis i rep informes de tornada dels mateixos zombis.

En un atac de força bruta el ciberatacant comprova sistemàticament totes les contrasenyes possibles fins que es troba la correcta.

Les *botnets*, l'eina multiusos del cibercrim

Les botnets són eines polivalents utilitzades per portar a terme diferents tipus d'atacs i accions malicioses.

Una *botnet* és un conjunt d'ordinadors o dispositius que un cibercriminal ha infectat mitjançant un codi maliciós i han quedat sota el seu control a través d'un servidor de control central C&C *(Command & Control)*. Mitjançant aquest, el cibercriminal pot controlar tota la *botnet* per portar a terme accions malicioses que, en el cas de disposar de milers de dispositius, poden causar grans impactes. Les *botnets* són eines polivalents utilitzades per realitzar diferents tipus d'atacs i accions malicioses.

Atacs DDoS. Tradicionalment, les *botnets* són utilitzades per perpetrar atacs DDoS amb l'objectiu de provocar la disrupció o caiguda d'un sistema informàtic enviant **més peticions al sistema de les que aquest pot suportar** i fent que aquest se saturi o caigui. Sorprèn constatar com, segons un estudi d'Spamhaus, el **50% dels atacs provenen de dispositius amb sistema operatiu Android i iOS** (veure il·lustració 6).

Correu brossa i *phishing*. Les *botnets* són responsables de l'enviament de gran quantitat de correus brossa i *phishing*. Tant és així que el correu brossa i el *phishing* actualment són més del **55% del tràfic de correu electrònic mundial**[20]. Un exemple d'actualitat és la *botnet* **Emotet***,* utilitzada en campanyes de *ransomware* d'abast mundial (veure capítol Ha estat notícia), la qual roba credencials i llistes de contactes de l'equip infectat per enviar nous correus de *phishing* amb un adjunt maliciós per tal que la *botnet* segueixi propagant-se**.**

Clics fraudulents. Quan una *botnet* conté dispositius que tenen navegador, com ara mòbils i ordinadors, aquests es poden usar per fer clics en anuncis col·locats en una pàgina web propietat del ciberdelinqüent, de manera que aquest obté ingressos de l'empresa anunciant. Segons la universitat de Twente (veure il·lustració 8), aquest pràctica pot generar beneficis de l'ordre de diversos milions de dòlars.

Atacs de força bruta. Les *botnets* es poden usar per tal de realitzar atacs de *força bruta* contra sistemes mentre es preserva l'anonimat de l'atacant. El juny de 2019, es va detectar la *botnet* anomenada Golbrute que va atacar **un milió i mig de servidors** a través del port d'escriptori remot o RDP[21].

[20] *https://securelist.com/correu brossa-and-phishing-in-q2-2019/92379/*
[21] *https://www.zdnet.com/article/a-botnet-is-brute-forcing-over-1-5-million-rdp-servers-all-over-the-world/*

Un bot es programa informàtic o mecanisme automatitzat que executa una tasca específica.

El DDoS (Distributed Denial of Service) és un atac originat per una xarxa de dispositius o botnet. L'objectiu és causar la indisponiblitat d'un servei i impedir-hi l'accés als usuaris legítims, amb la saturació del tràfic i el processat computacional que els servidors són capaços de suportar.

Un estressador d'IP o IP stresser és un sistema dissenyat per a provar la robustesa d'un servidor web o d'una xarxa amb l'objectiu que l'administrador pugui determinar si els recursos existents són adequats i funcionen correctament.

Un servei d'atacs DDoS o booter ofereix atacs de denegació de servei distribuïts, amb l'objectiu d'afectar el funcionament correcte de servidors web i xarxes.

Mineria. Una *botnet* pot **utilitzar els recursos computacionals dels seus *bots*** per a la mineria de criptomonedes. Aquest agost passat, **la *botnet* Smominru ha ressorgit**, usada per activitats com el *cryptojacking*[22]. Anteriorment, Smominru havia assolit una mida de més de **500.000 bots** i se li atribueixen uns guanys de més de **2.3 milions de dòlars**[23].

Dropper. Algunes *botnets,* un cop tenen el control del *bot*, tenen capacitat per **forçar la descàrrega de nou *malware***. En el cas de les campanyes de *ransomware* recents, la *botnet* **Emotet força la descàrrega de Trickbot, el *malware* d'una nova *botnet*** que permet que els ciberatacants accedeixin als sistemes de la víctima.

Escaneig de xarxa. Els cibercriminals utilitzen les *botnets* per escanejar la xarxa amb l'objectiu d'**identificar ports, vulnerabilitats i sistemes no actualitzats o mal configurats**. Després de la fase d'escaneig, el ciberatacant podrà focalitzar el seu esforç per atacar els sistemes més vulnerables. Es dona el fet que, segons Verizon, **un 77% dels atacs contra serveis web són automatitzats a través de *botnets***[24].

El negoci de les *botnets*

El servei de moltes d'aquestes *botnets* pot contractar-se fàcilment, com qualsevol altre servei en línia, a preus assequibles, especialment si es té en compte que poden causar danys molt importants. Un estudi del 2018 de la **Universitat de Twente** calculava com de lucrativa pot arribar a ser l'explotació comercial d'una *botnet* en funció de l'activitat a la qual es dediqui.

	Atac DDoS	Frau bancari	Correu brossa	Frau de clics
Malware	variant de Mirai*	Zeus	?	ZeroAccess
Nombre de *bots*	30.000 bots	30.000 bots	10.000 bots	140.000 bots
Cost del paquet de *malware*	-$30	-$700 a -$10.000	?	-$700 a -$10.000
Cost de distribució (PPI = 0,0935 $)**	-$2.805	-$2.805	-$935	-$13.090
Cost del *hosting bulletproof*	-$2.400	-$70	-$2.400	-$70
Manteniment	?	-$5.167	?	?
Màrqueting	-$2.400	-$2.400	?	?
Ingressos mensuals	$26.000	$18.800.000	$300.000	$25.000.000
Cost del moviment dels diners (3% de comissió)	-$780	-$564.000	-$9.000	-$750.000
Beneficis mensuals aproximats	**~20 K$**	**~18 M$**	**~290 K$**	**~24 M$**

* El codi de Mirai es va fer públic el 2016 i és habitual l'aparició de noves variants.
** PPI = Pagament per Infecció; es considera que els *bots* s'han de reinfectar cada mes.

Il·lustració 8. Anàlisi cost/benefici mensual derivat de l'explotació d'una botnet[25]

Segons aquest estudi, **construir una *botnet* per realitzar atacs DDoS és la menys lucrativa de les opcions**. Es poden trobar a Internet amb el terme *IP Stresser* o *booter* i, per menys de 10 dòlars (en criptomoneda), és possible contractar l'ús d'una *botnet* per fer atacs de denegació de servei[26]. Amb una *botnet* de 10.000 *bots*, l'**enviament de correu brossa** és una activitat més lucrativa que el DDoS i podria

[22] *https://www.csoonline.com/article/3439400/secrets-of-latest-smominru-botnet-variant-revealed-in-new-attack.html*
[23] *https://www.bleepingcomputer.com/news/security/smominru-mining-botnet-in-cyber-turf-war-with-rival-malware/*
[24] *https://enterprise.verizon.com/resources/reports/dbir/*
[25] *https://arxiv.org/pdf/1804.10848.pdf*
[26] *https://www.stressthem.to/#pricing*

El phishing és un atac d'enginyeria social en el qual l'atacant imita una organització de confiança simulant l'entorn habitual d'interacció que l'usuari tindria (pàgina web, correu electrònic, aplicació, etc.). L'objectiu del phishing és enganyar l'usuari i obtenir-ne un benefici econòmic o una informació determinada

El correu brossa o spam és Conjunt de missatges electrònics importuns, generalment de caràcter publicitari i sense interès per al receptor, que s'envien indiscriminadament a un gran nombre d'internautes.004

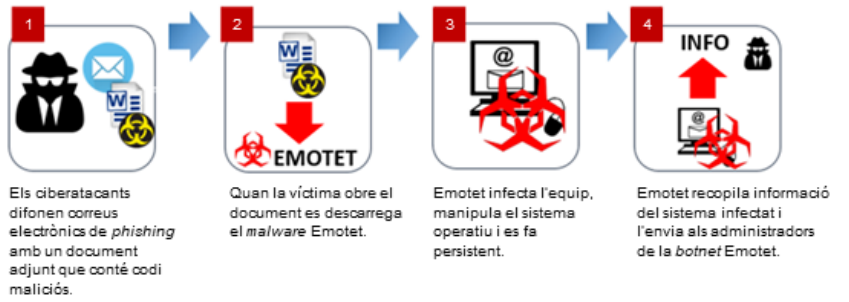
reportar uns **290.000 dòlars mensuals**. El frau de clics, amb l'ús de 140.000 bots, és capaç de reportar uns sorprenents 20 milions de dòlars mensuals. Destaca el frau bancari com l'activitat clarament més lucrativa, amb 18 milions de dòlars al mes que equivalen a 600 dòlars per *bot*.

Destaca el frau bancari com l'activitat clarament més lucrativa, amb 18 milions de dòlars al mes que equivalen a 600 dòlars per bot.

Incorporació del *ransomware*

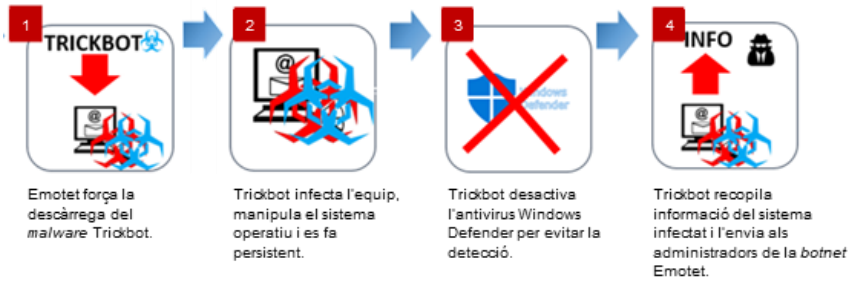
Les *botnets* constitueixen un mecanisme de distribució ideal per a molts tipus d'atacs. D'altra banda, el *ransomware* dirigit és una eina molt efectiva pels criminals a l'hora de lucrar-se. Ha estat qüestió de temps que el cibercrim aconseguís unir el millor de cada tècnica d'atac per aconseguir maximitzar la difusió de *ransomware* i possibilitar campanyes d'abast global contra un gran nombre d'objectius. **Emotet, Trickbot** i **Ryuk**, junts, constitueixen una autèntica **triple amenaça**.

En una primera fase, s'infecta la víctima amb el *malware* de tipus *botnet* **Emotet** mitjançant campanyes de *phising* o correu brossa. D'aquesta manera, **l'equip infectat passa a formar part d'una xarxa de dispositius sobre els quals el cibercriminal disposa d'accés i control**.



Il·lustració 9. Primera fase de l'atac amb la triple amenaça: Emotet

En una segona fase, l'operador de la *botnet* **Emotet** força la descàrrega de **Trickbot**, un nou *malware* de tipus *botnet* per encàrrec d'un nou actor cibercriminal a canvi d'un pagament per infecció o PPI (veure il·lustració 8). Així, **el nou actor cibercriminal obté el control dels equips infectats** i ja està preparat per la darrera fase de l'atac.



Il·lustració 10. Segona fase de l'atac amb la triple amenaça: Trickbot

Finalment, a partir de l'equip infectat, els cibercriminals es desplacen per la xarxa de l'organització de la víctima, fent ús de tècniques de desplaçament lateral, escalada de privilegis i captura de credencials. Els ciberatacants procuraran **obtenir un esquema de la xarxa a atacar amb l'objectiu de localitzar els sistemes més crítics** on desplegar el *ransomware*.

Il·lustració 11. Tercera fase de l'atac amb la triple amenaça: Ryuk

Aquesta triple amenaça ha estat responsable de les campanyes més importants dirigides contra organitzacions i empreses, tot i que altres també han utilitzat mecanismes similars basats en la utilització combinada de *botnets* i *ransomware*. Així, també ha tingut un gran impacte la utilització de la ***botnet* Dridex**, la qual **es propaga mitjançant Emotet o falses actualitzacions del navegador web** i**,** en darrera instància, s'utilitza per a desplegar el ***ransomware* Bitpaymer**.

Proliferació de les *botnets*

La mida de les *botnets* varia amb el temps a causa de les actualitzacions de seguretat, els antivirus i el *firmware* dels dispositius, però s'estima que alguns casos han arribat a tenir una mida **d'uns dos milions i mig de dispositius**[27]. Una bona part d'aquests dispositius són *webcams* o dispositius *IoT* desactualitzats, mal configurats o amb pobres mesures de ciberseguretat de fàbrica.

El firmware o microprogramari és el software que té interacció amb el maquinari, essent l'encarregat de controlar-lo per executar correctament les ordres externes.

En qualsevol cas, els darrers temps s'observa un creixement continu en el nombre de *botnets* creades (veure il·lustració 4). Dins d'aquest creixement, les campanyes que fan ús del binomi de *botnets* **Emotet** i **Trickbot** tenen una rellevància especial i, de fet, aquest trimestre s'han detectat **614 noves *botnets* de Trickbot** i **162 d'Emotet** (**19,8% del total**)[28].

Tot i que **Emotet i Trickbot** han obtingut un ressò especial als mitjans de comunicació, la *botnet* més detectada és **Lokibot**, especialitzada en robar credencials bancàries a sistemes **Windows** i que, com **Emotet**, es distribueix mitjançant l'enviament de correu brossa[29].

[27] *https://retina.elpais.com/retina/2018/03/21/tendencias/1521633331_604101.html*
[28] *https://www.spamhaus.org/news/images/Q3-2019/2019-Q3-Spamhaus-Botnet-Threat-Update.pdf*
[29] *https://blog.malwarebytes.com/detections/trojan-trickbot/*

Fets rellevants

- **Imperva**, referent mundial en la protecció contra atacs DDoS de sistemes informàtics, ha fet públic que el juliol va detectar un atac DDoS des de **400.000 dispositius IoT** que va ser capaç de **generar més de 292.000 peticions per minut a una pàgina web**[30]**.**

- A l'agost, diversos investigadors van descobrir que una *botnet* anomenada **Neutrino** va estar escanejant i apoderant-se de diversos servidors, **aprofitant els accessos que havien deixat altres *malware* amb anterioritat**[31].

- Al mes d'agost es va descobrir una **nova *botnet*** formada per dispositius ***IoT* Android** que aprofita la **mala praxi d'alguns fabricants de deixar serveis oberts i sense necessitat d'autenticació** per a connectar-s'hi. Els dispositius infectats ja es compten per milers.[32]

- Segons un informe d'ESET, la *botnet* anomenada **GoBotKr** dirigia atacs a fans de Korean TV, **comprometent dispositius mitjançant còpies pirata de pel·lícules i jocs a través de pàgines "torrent"**. La motivació principal de la *botnet* és **realitzar atacs *DDoS***[33].

- Al setembre, diversos ajuntaments de la província de **Lleida** van ser víctima del *malware* **Emotet**, propagat mitjançant la *botnet* del mateix nom[34].

- Una campanya d'**Emotet**, **Trickbot** i **Ryuk** va afectar diverses organitzacions públiques al país basc, els incidents estan sent investigats per l'**Ertzaintza**[35].

- A finals de trimestre, l'**Ajuntament d'Aljaraque**, a **Huelva**, va detectar correus amb documents **Word** adjunts que forçaven la descàrrega d'**Emotet**, però no es va fer pública la repercussió de l'atac[36].

- Aquest setembre, la policia francesa va aconseguir intervenir una *botnet* de més de **850.000 dispositius** que s'usava per a la mineria de criptomonedes[37].

- Es va detectar el ressorgiment de la *botnet* **Smominru**, que ataca màquines **Windows**, instal·la un troià per propagar-se per la xarxa i un *software* de criptomineria. Per comprometre les màquines utilitza el famós exploit **EternalBlue** i atacs per *RDP*[38].

- Al setembre es va descobrir una campanya de *phishing* en la qual se **suplantava l'organisme d'hisenda dels EUA** informant les víctimes que eren elegibles per a una devolució d'impostos. Quan l'usuari ingressava a la pàgina falsa i es descarregava el formulari de devolució d'impostos, **es descarregava també un programa que afegia l'ordinador a una *botnet***[39].

[30] *https://www.bankinfosecurity.com/massive-botnet-attack-used-more-than-400000-iot-devices-a-12841*
[31] *https://www.zdnet.com/article/a-botnet-has-been-cannibalizing-other-hackers-web-shells-for-more-than-a-year/#ftag=RSSbaffb68*
[32] *https://www.darkreading.com/attacks-breaches/new-botnet-targets-android-set-top-boxes/d/d-id/1335688?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple*
[33] *https://threatpost.com/gobotkr-pirate-torrents-ddos-botnet/146285/*
[34] *https://www.segre.com/noticies/comarques/2019/09/25/suplanten_mails_ajuntaments_lleida_per_propagar_virus_informatics_87532_1091.html*
[35] *https://www.noticiasdegipuzkoa.eus/2019/10/01/sociedad/un-ataque-masivo-de-emails-con-virus-afecta-a-multiples-entes-publicos-vascos*
[36] *https://www.europapress.es/andalucia/huelva-00354/noticia-ayuntamiento-aljaraque-huelva-denuncia-ataque-virus-informatico-20191002184916.html*
[37] *https://techcrunch.com/2019/09/01/police-botnet-takedown-infections/*
[38] *https://www.guardicore.com/2019/09/smominru-botnet-attack-breaches-windows-machines-using-eternalblue-exploit*
[39] *https://www.securityweek.com/phishing-emails-deliver-amadey-malware-us-taxpayers*


18:42:18.018", "deltaStartMillis":
ndlers.RequestHandler", "method":"handle",
ge":"Duration Log", "durationMillis":"508"}{"
e", "webParams":"null", "class":"com.orgmanag
46ac-9745-839146a20f09", "sessionID":"144o2n6
mestamp":"2017-06-03T18:43:335.030", "deltaSta
a_new.json", "class":"com.orgmanager.handlers
rnd3s3n7wg0k", "sizeChars":"48455", "message"
vel":"INFO", "webURL":"/app/page/report", "w
4e7d-8047-498454af885d", "sessionID":"144o2n
stamp":"2017-06-03T18:46:921.000", "deltaSta
dlers.RequestHandler", "method":"handle", "
ge":"Duration Log", "durationMillis":"10"}{"
le", "webParams":"file=chartdata_new.json",
4a60-88d7-6ead86e273d1", "sessionID":"144o2n
estamp":"2017-06-03T18:42:18.018", "deltaSta
dlers.RequestHandler", "method":"handle",
e":"Duration Log", "durationMillis":"508"}{"
", "webParams":"null", "class":"com.orgmanag
6ac-9745-839146a20f09", "sessionID":"144o2n6
estamp":"2017-06-03T18:43:335.030", "deltaSta
_new.json", "class":"com.orgmanager.handlers
nd3s3n7wg0k", "sizeChars":"48455", "message"
vel":"INFO", "webURL":"/app/page/report", "w
4e7d-8047-498454af885d", "sessionID":"144o2n
stamp":"2017-06-03T18:46:921.000", "deltaSta
dlers.RequestHandler", "method":"handle",

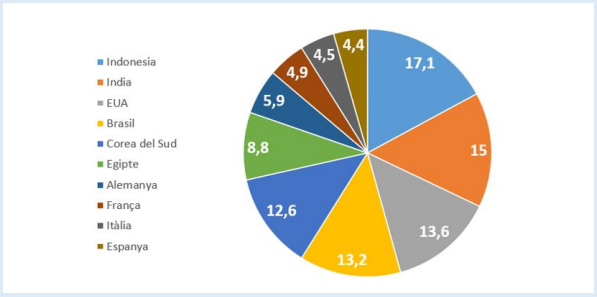
Ransomware dirigit

Baròmetre

Aquest tercer trimestre de 2019 ha destacat per l'increment dels atacs de *ransomware* i, en especial, aquells dirigits contra el sector públic, concretament contra el sector educatiu coincidint amb l'inici del curs escolar.

Països afectats

El portal ID Ransomware d'Emsisoft, dirigit a donar suport a les víctimes de *ransomware*, ha analitzat 230.000 peticions d'usuaris particulars i empreses per identificar els països d'origen.

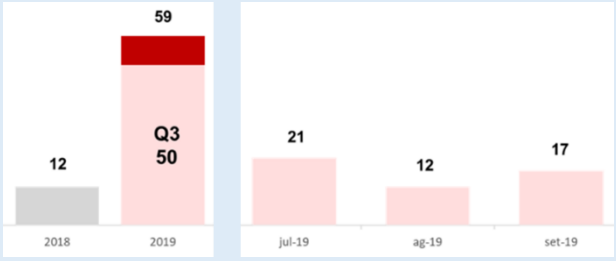


Il·lustració 12. Països més atacats per ransomware[40]

Espanya és el desè país des d'on s'informen més infeccions per *ransomware* amb una mitjana de 56 peticions de suport al dia els darrers 6 mesos.

Sector educatiu

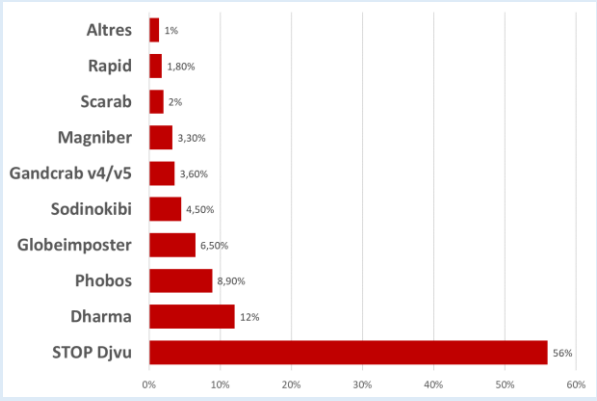
Les empreses són les grans damnificades pel *ransomware*, però els atacs al sector públic segueixen una tendència creixent. Aquest darrer trimestre, coincidint amb els períodes de matriculació i inici de classes, els centres educatius han estat les víctimes predilectes dels ciberatacants.



Il·lustració 13. Casos de ransomware *contra districtes escolars als EUA*[41]

Top *ransomware*

El mateix estudi d'Emisoft identifica les famílies de *ransomware* més detectades.

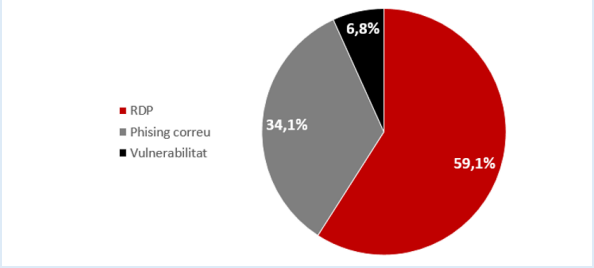


Il·lustració 14. Ransomware *més detectats el 3r semestre*[42]

El *ransomware* més detectat, STOP, es difon mitjançant *software* generador de claus de desbloqueig (*keygen*) i pirateig de programari. Ara bé, la resta dels *ransomware* més detectats es difonen amb atacs dirigits. Cal destacar que no s'hi troba Ryuk, tot i ser responsable d'atacs contra grans organitzacions causants de grans impactes. Segons Coveware, la mida mitjana de les empreses afectades per Ryuk és de 3.187 treballadors[43].

Els principals vectors d'atac

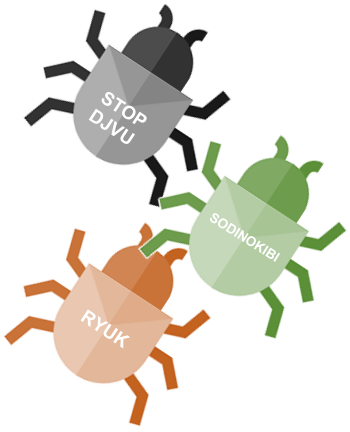
S'han identificat els següents vectors d'atac com els principalment usats en els atacs dirigits de *ransomware*. Principalment, l'atacant sol aprofitar un accés RDP, infecta les víctimes amb *phishing* o explota una vulnerabilitat no solucionada a temps.



Il·lustració 15. Principals vectors d'atac a un sistema informàtic per comprometre'l amb ransomware[44]

[40] *https://blog.emsisoft.com/en/34335/ransomware-statistics-for-2019-q2-to-q3-report/*
[41] *Font: Agència de Ciberseguretat de Catalunya*
[42] *https://blog.emsisoft.com/en/34335/ransomware-statistics-for-2019-q2-to-q3-report/*
[43] *https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread*
[44] *https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread*

Ransomware dirigit



Una família és un conjunt de programaris maliciosos que comparteixen una part substancial de codi original i inconfusible.

Una variant és una peça de programari maliciós creada a partir de la modificació del codi d'una família específica i coneguda.

Un generador de claus és un programa informàtic que s'utilitza per a generar una clau que permet desbloquejar un programa o un conjunt de dades per tal d'accedir-hi.

Un crac és un programari utilitzat per a desactivar els sistemes de protecció d'una aplicació o d'un programari determinat, a fi de poder-los utilitzar o distribuir fraudulentament.

Campanyes de *ransomware* dirigit

Els darreres mesos han estat protagonitzats per diverses campanyes de *ransomware.* Al darrere hi ha diferents actors cibercriminals, cada un amb tècniques i codis de *ransomware* propis, però tots tenen en comú que han identificat i comparteixen una activitat criminal molt lucrativa.

En el podi de les famílies de *ransomware* més detectades (veure il·lustració 14) s'hi troba **STOP DJVU**, el qual es propaga a través de generadors de claus i cracs descarregats d'Internet. Els següents *ransomware* més detectat són **Dharma** i la seva variant **Phobos** i destaquen pel fet que, en cas de pagament del rescat, l'eina de desxifrat lliurada pels ciberdelinqüents és poc òptima i pot arribar a trigar 8 dies per recuperar la informació xifrada, dos dies més que la mitjana dels *ransomware*[45].

Cal fer una menció específica al *ransomware* **Sodinokibi**, una variant del famós Gandcrab i que utilitza el mateix model de distribució RaaS (*Ransomware as a Service*) a través de diferents actors associats. Cal recordar que els operadors de Gandcrab, abans de cessar la seva activitat, van fer ostentació dels més de **2.000 milions de dòlars recaptats** per tota la xarxa criminal d'associats[46].

Els *ransomwares* Ryuk, Bitpaymer i Megacortex no figuren entre els més detectats, però són responsables dels principals incidents i de causar els impactes més importants. **Ryuk** i **Bitmpaymer** es caracteritzen per fer ús de les *botnets* Trickbot i Dridex, respectivament, per penetrar a la xarxa de la víctima, identificar i executar el *ransomware* on major dany pugui causar (veure capítol *Botnets*)[47 i 48]. **Megacortex** destaca perquè ha estat utilitzat en campanyes dirigides a empreses d'Europa i els EUA, en les quals s'han arribat a demanar rescats de fins a 5,8 milions de dòlars[49].

Atacs d'escriptori remot (RDP)

Els atacs per RDP suposen més del 59% dels atacs quan es té la intenció d'infectar un sistema amb ransomware.

L'atac a través de les connexions a **escriptori remot** (RDP) **ha esdevingut la manera preferida dels ciberdelinqüents per tal de comprometre els sistemes d'informació de les empreses i infectar-los mitjançant *ransomware***. Tan és així que els atacs per RDP suposen el 59% dels atacs amb *ransomware*[50] (veure il·lustració 15).

[45] *https://www.coveware.com/*
[46] https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/
[47] *https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data*
[48] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/
[49] *https://www.accenture.com/us-en/blogs/blogs-megacortex-business-disruption*
[50] *https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread*

Un port és una via d'entrada i sortida de les dades en un sistema informàtic.

Una porta del darrere o backdoor és un mecanisme que fa possible l'accés a una aplicació evitant les restriccions i les mesures de seguretat, sempre que se'n conegui l'existència i el funcionament.

Una exploit és un programa que aprofita la vulnerabilitat d'un dispositiu o sistema per a introduir-hi programari maliciós.

Un pedaç és un fitxer que conté una o diverses modificacions d'un programa destinades a corregir-ne un error, a incorporar-hi funcions noves o a actualitzar-lo.

RDP (Remote Desktop Protocol) *és un protocol propietari desenvolupat per Microsoft que permet la comunicació en l'execució d'una aplicació entre una terminal (mostrant la informació processada que rep del servidor) i un servidor de qualsevol tecnologia (rebent la informació donada per l'usuari al terminal mitjançant el ratolí o el teclat). La configuració per defecte utilitza el port 3389 per a comunicar els terminals amb el servidor de destinació.*

El temps mitjà per tal que un servidor amb el port RDP obert sigui detectat és de poc més de 3 hores i mitja.

El fet és que les eines per la cerca de sistemes amb el port RDP obert i per realitzar atacs de força bruta, han demostrat ser molt efectives. En aquesta línia, gràcies a l'ús de buscadors com **Shodan** o d'eines d'escaneig com **NMap, Masscan** o **RdpScan**, el **temps mitjà per tal que un servidor amb el port *RDP* obert sigui detectat és de poc més de 3 hores i mitja**, tot i que en alguns casos s'ha fet en menys d'un minut i mig[51].

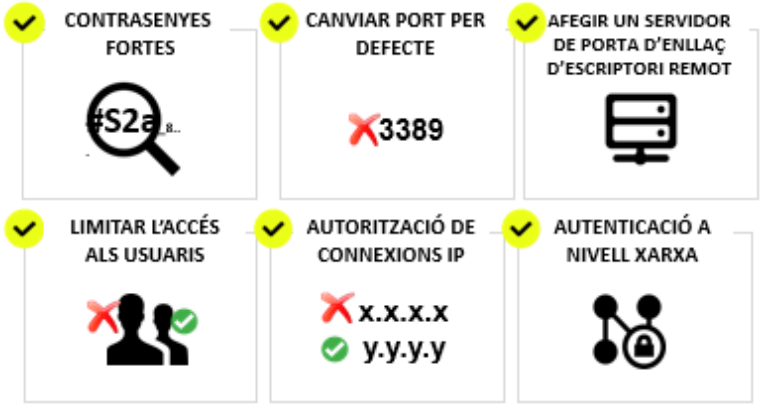
Quan un atacant troba un servidor amb el port *RDP* obert, pot intentar **accedir al sistema mitjançant atacs de força bruta amb credencials comprades a la *dark web*** o **obtingudes mitjançant enginyeria social.** Per realitzar un atac de força bruta, existeix un ampli ventall d'eines com **John the Ripper, Rainbow crack, Cain and Abel, Ophcrack**, etc.

Un fet que ha promogut els atacs via RDP ha estat el descobriment, el darrer mes de maig, de la **vulnerabilitat Bluekeep que afecta sistemes antics de Microsoft**[52] (Windows XP, Windows 7, Windows Server 2003, Windows Server 2008 i Windows 2008 Server R2). Aquesta vulnerabilitat permet accedir als sistemes mitjançant una porta del darrere sense necessitat de conèixer les credencials d'accés. Fins i tot va aparèixer un *exploit* que els cibercriminals han aprofitat per comprometre sistemes on encara no s'ha aplicat el pedaç de seguretat.

Mesures preventives

Malgrat la virulència dels atacs de *ransomware*, existeixen diverses mesures preventives dirigides a protegir-se de cada un dels principals vectors d'atac (veure il·lustració 15).

Contra els atacs per RDP. Si inhabilitar el port RDP no és una opció, encara es poden prendre una sèrie de mesures preventives per evitar l'accés als atacants.



Il·lustració 16. Mesures preventives contra els atacs per RDP

[51] *https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-rdp-exposed-the-threats-thats-already-at-your-door-wp.pdf*
[52] *https://www.welivesecurity.com/la-es/2019/06/10/bluekeep-vulnerabilidad-tiene-vilo-industria-seguridad/*

Contra el *phising*. Es poden prendre mesures diverses per contrarestar els atacs d'enginyeria social que pretenen explotar el factor humà.

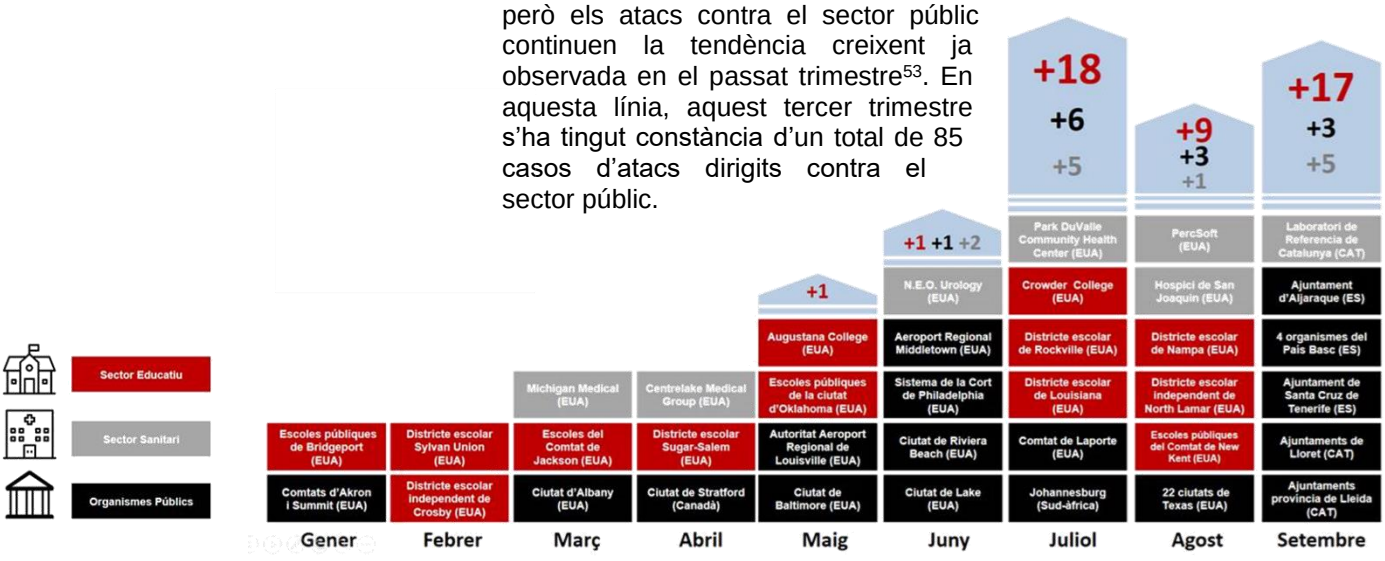
Il·lustració 17. Mesures preventives contra les atacs de phising

Contra l'explotació de vulnerabilitats. Cal utilitzar sistemes ben protegits, actualitzats i monitorar-los continuadament.

Il·lustració 18. Mesures preventives contra els atacs per explotació de vulnerabilitats

Atacs dirigits contra el sector públic

El teixit empresarial és el més afectat pels atacs de *ransomware* dirigits, però els atacs contra el sector públic continuen la tendència creixent ja observada en el passat trimestre[53]. En aquesta línia, aquest tercer trimestre s'ha tingut constància d'un total de 85 casos d'atacs dirigits contra el sector públic.



Il·lustració 19. Atacs de ransomware *contra institucions públiques*[54]

[53] *https://ciberseguretat.gencat.cat/web/.content/PDF/InformeTendenciesT22019.pdf*
[54] *Dades recollides per l'Agència de Ciberseguretat de Catalunya*

Sector educatiu. En el sector públic, el sector educatiu ha estat l'àmbit més afectat pel *ransomware* aquest tercer trimestre i, només a causa dels atacs als districtes escolars i organismes educatius dels EUA, **més de 500 escoles i universitats han confirmat que han estat afectades per atacs de *ransomware***[55], tot i que poden ser encara més nombroses, ja que no tots els incidents es fan públics[56]. **Amb l'objectiu de forçar el pagament del rescat per recuperar l'activitat ràpidament, els atacs s'han concentrat uns pocs dies abans de l'inici escolar**, un període d'intensa activitat acadèmica a causa de les inscripcions de l'alumnat.

Organismes públics. Un nombre important dels atacs d'aquest trimestre han estat dirigits contra organismes i institucions públiques. Diversos exponents d'aquesta tendència es poden observar en l'onada d'atacs amb Emotet s'han vist afectats diversos ajuntaments i organitzacions públiques catalanes i espanyoles (veure capítol *Ha estat notícia*).

Sector sanitari. Els atacs no es limiten a hospitals i clíniques, sinó també a organitzacions que formen part de la seva cadena de subministrament. Els atacants entenen que els organismes d'aquest sector tendeixen a posicionar-se a favor de pagar el rescat, ja que una pèrdua de dades podria posar vides humanes en perill. Per incrementar encara més la pressió a pagar el rescat, en alguns casos el preu del rescat s'incrementa de forma progressiva: com més es triga a pagar, més alt és el seu cost[57].

Il·lustració 20. Rescat de ransomware *on el preu canvia al cap d'un temps*

[55] *https://www.infosecurity-magazine.com/news/hundreds-of-us-schools-hit-by/*
[56] *https://securityboulevard.com/2019/10/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/*
[57] *https://blog.malwarebytes.com/detections/ransom-sodinokibi/*

Fets rellevants

- El juliol de 2019, l'Ajuntament de **Baltimore** (EUA) va decidir dedicar **10 milions de dòlars addicionals** als **18 milions computats inicialment** per a poder combatre l'atac de *ransomware* que havia patit el passat mes de maig i pel qual els cibercriminals demanaven **80.000 dòlars de rescat**[58].

- Addicionalment, Baltimore vol contractar una assegurança contra futurs atacs de *ransomware* de **20 milions de dòlars**. L'assegurança costaria a la ciutat **830.000 dòlars l'any**[59].

- **Eurofins**, l'empresa d'anàlisi forense més important del **Regne Unit**, va fer públic aquest mes de juliol passat que va pagar un rescat per un atac de *ransomware* que va patir el més de juny[60].

- A l'agost, **22 ciutats** de **Texas** (EUA) van ser atacades de forma simultània amb un **atac coordinat** del qual no s'han fet públics més detalls però que deixen palesa l'oportunisme que són capaços d'assolir els atacants[61].

- L'atac a la ciutat de **New Bedford** (EUA) del juliol va destacar per haver rebut una petició de rescat desproporcionada de **5,3 milions de dòlars**[62].

- Al districte escolar de **Monroe** (Nova York), un total de **49 escoles** van ser víctimes de *ransomware* el dia **3 de setembre, cosa que va obligar a ajornar l'inici del curs escolar previst pel dia 4**[63].

- El districte escolar de **Wallenpaupack** va ser víctima, aquest mes de setembre, d'un atac per *ransomware* que **va paralitzar 3.000 ordinadors**. Aquest *ransomware* és el segon atac informàtic que viu el districte escolar aquest any[64].

- Aquest setembre, el **departament de Comunicacions, acció climàtica i medi ambient** del govern d'**Irlanda** va reconèixer que l'any 2018 havia estat víctima d'un atac per *ransomware*[65].

- El 6 de setembre, les escoles públiques de **Rockford** (EUA) van viure un atac de *ransomware* que va causar talls als sistemes informàtics. El districte es va negar a compartir més detalls[66].

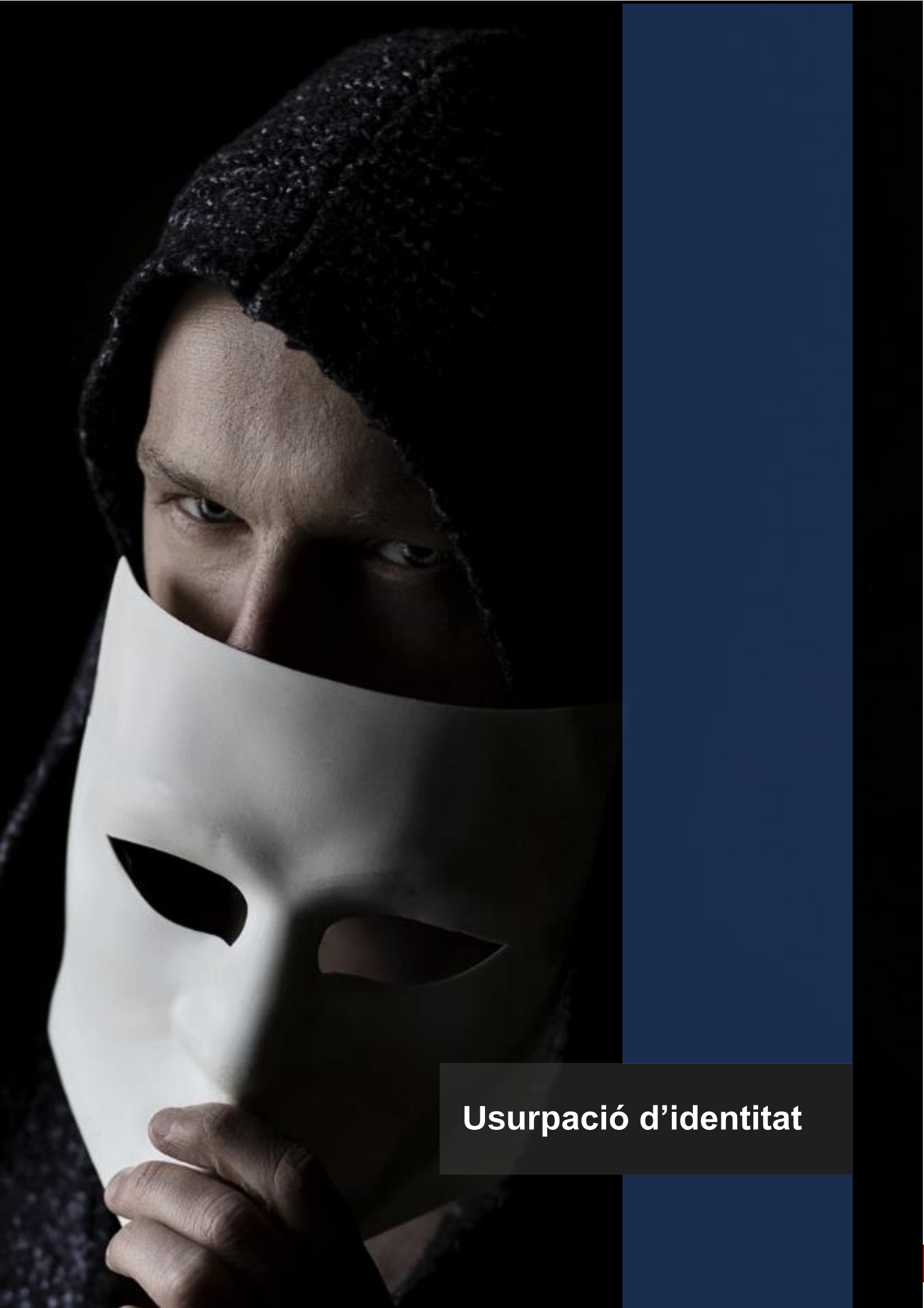
- El comtat d'**Orange**, a **Nova York** (EUA), va haver d'**endarrerir l'inici del curs** escolar a causa de l'atac per *ransomware* que han patit a principis del mes de setembre i que va afectar 49 escoles[67].

- Les escoles de **Flagstaff** (EUA) van haver de **suspendre el curs escolar** a causa de l'atac de *ransomware* que van patir el 4 de setembre[68].

- Les escoles del **comtat de Mobile** (EUA) van ser víctimes d'un atac de *ransomware* **contra un dels seus proveïdors**, fet que va provocar la **caiguda de la seva pàgina web**[69].

- El projecte **NoMoreRansom**, del qual l'Agència de Ciberseguretat de Catalunya n'és membre, va fer públic que ja ha evitat guanys dels atacants per valor de més de **108 milions de dòlars**[70].

[58] *https://hotforsecurity.bitdefender.com/blog/baltimore-allocates-10-million-to-emergency-funding-in-wake-of-ransomware-attack-21372.html*
[59] *https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/baltimore-recovery-update/*
[60] *https://www.bbc.com/news/uk-48881959*
[61] *https://www.nytimes.com/2019/08/20/us/texas-ransomware.html*
[62] *https://www.govtech.com/security/Ransomware-Hacker-Demands-53-Million-of-New-Bedford-Mass.html*
[63] *https://www.darkreading.com/threat-intelligence/ransomware-strikes-49-school-districts-and-colleges-in-2019/d/d-id/1335872*
[64] *https://www.neagle.com/news/20190913/school-district-computers-paralyzed-in-attack*
[65] *https://www.thetimes.co.uk/edition/ireland/irish-government-admits-ransomware-breach-s8n6nxpgj*
[66] *https://www.databreaches.net/ransomware-caused-outages-at-rps-205-could-last-days/*
[67] *https://www.databreaches.net/ny-school-delays-start-of-year-after-ransomware-attack/*
[68] *https://www.databreaches.net/school-officials-ransomware-prompts-school-closure-in-flagstaff/*
[69] *https://www.al.com/news/mobile/2019/09/mobile-county-school-district-website-down-after-ransomware-attack.html*
[70] *https://www.zdnet.com/article/no-more-ransom-project-has-prevented-ransomware-profits-of-at-least-108-million/#ftag=RSSbaffb68*



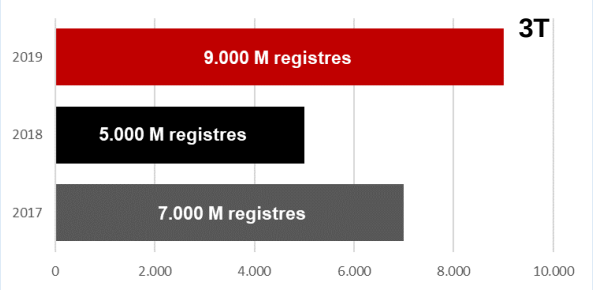
Usurpació d'identitat

Baròmetre

Les pàgines web visitades, què es compra, cerques, xarxes socials... El rastre d'informació personal que es troba a Internet pot ser utilitzat per perpetrar accions criminals contra els usuaris de les xarxes per mitjà del robatori o usurpació.

Fuites de dades

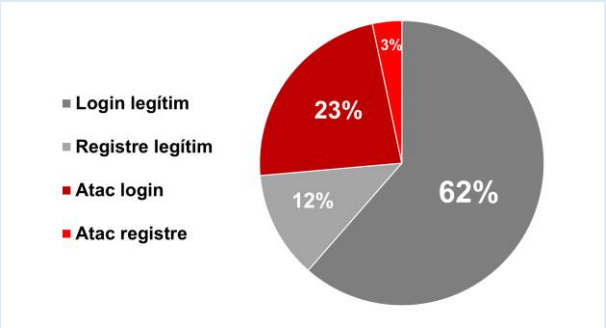
Les fuites de dades són una de les fonts principals d'informació dels cibercriminals i són un mecanisme d'obtenció de dades personals, credencials i altres tipus d'informació utilitzada en usurpacions d'identitat. Durant el 3r trimestre de 2019 el nombre de registres amb informació personal filtrats ja superen els anys anteriors complets.



Il·lustració 21. Evolució de la quantitat de registres filtrats des de 2017[71]

Atacs a les xarxes socials

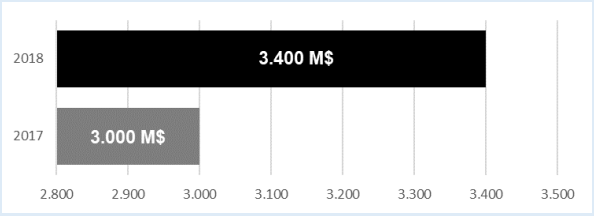
Les xarxes socials són objectiu de continus intents d'atac per a la suplantació d'identitat. En alguns casos es pretén robar el compte de la víctima amb atacs de força bruta o fent ús de credencials obtingudes en fuites de dades prèvies (atacs de *login*). En altres casos es creen comptes fraudulents per suplantar l'original (atac de registre). En conjunt, aquestes activitats representen un 26% d'intents d'accés fraudulent.



Il·lustració 22. Transaccions de login *i registre a les xarxes socials*[72]

Creix el frau econòmic

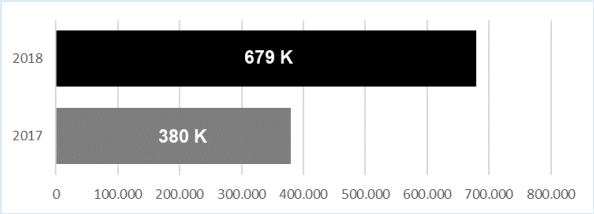
La suplantació és un mecanisme que pot permetre que els cibercriminals obrin comptes bancaris fent-se passar per les víctimes amb l'objectiu d'obtenir targetes de crèdit o préstecs econòmics. Sota aquest tipus de suplantació d'identitat, els cibercriminals van ser capaços de robar 3.400 milions de dòlars l'any 2018.



Il·lustració 23. Evolució de la quantitat econòmica defraudada als bancs mitjançant la suplantació d'identitat (M$)[73]

Creixen els segrests de línies mòbils

El segrest de línies mòbils mitjançant tècniques com el *SIM swapping* (enganyar l'operador de telecomunicacions per aconseguir transferir la línia a una nova targeta SIM) és una pràctica creixent que persegueix l'objectiu de controlar el telèfon mòbil de la víctima per poder esquivar el control de doble autenticació dels comptes de la víctima. Si el criminal obté les credencials i la línia mòbil de la víctima, no tindrà cap impediment per fer el que vulgui. El 2018, el nombre de línies sota el control dels cibercriminals ja van doblar les xifres de 2017 i s'espera que així seguirà.



Il·lustració 24. Evolució del nombre de línies mòbils segrestades[74]

El mateix CEO de Twitter va alertar del *SIM swapping* i de la necessitat de prendre precaucions arran del *hackeig* del propi compte de Twitter.

[71] *https://www.riskbasedsecurity.com/*
[72] *https://www.nexusguard.com/threat-report-q1-2019*
[73] *https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt*
[74] *https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brun*

Usurpació d'identitat

Objectiu: les dades personals

Per **dada personal** s'entén qualsevol **informació que permeti diferenciar o fer seguiment de la identitat d'un individu**, com nom, cognoms, DNI, nom dels familiars, o qualsevol altra informació que pugui associar-s'hi, com dades mèdiques, bancàries, laborals o d'educació.

La identitat dels usuaris es troba digitalitzada a Internet i, si no es prenen les mesures de protecció adequades, pot ser robada amb l'objectiu de cometre algun tipus de frau o robatori

El rastre digital a la xarxa defineix els usuaris. A partir de les cerques realitzades s'identifiquen les seves preferències, les dades GPS dels telèfons permeten saber la ubicació, les galetes donen a conèixer els hàbits i les xarxes socials permeten obtenir tota mena d'informació sobre la persona, la seva feina, família, amistats, etc. D'aquesta manera, **la identitat dels usuaris es troba digitalitzada a Internet i, si no es prenen les mesures de protecció adequades, pot ser robada amb l'objectiu de cometre algun tipus de frau o robatori.**

Els incidents del darrer trimestre deixen palès com es pot obtenir accés a aquesta informació personal, si és necessari, utilitzant mètodes il·lícits: enganys a les víctimes per mitjà de tècniques d'enginyeria social, recopilació d'informació de les xarxes socials, realitzant ciberatacs dirigits allà on les dades estan emmagatzemades o bé comprant-les a la *dark web*.

Usurpació d'identitat a les xarxes socials

La usurpació d'identitat a les xarxes socials s'esdevé quan un ciberatacant s'apropia del compte d'usuari (Facebook, Instagram, Whatsapp, etc.) d'una altra persona o en crea un de fraudulent per fer-se passar per ella sense autorització. Aquest tercer trimestre s'ha observat un **clar augment del robatori de comptes de xarxes socials** (veure apartat Fets rellevants), i molts afecten **personatges famosos o entitats rellevants amb el corresponent ressò als mitjans de comunicació**.

Aquest trimestre han estat especialment rellevants els casos en què s'ha utilitzat l'**enginyeria social per aconseguir el control del compte d'usuari de la víctima,** especialment Whatsapp i Twitter (veure il·lustració 25). Per evitar que això succeeixi, cal mantenir la màxima de **no compartir cap tipus de contrasenya o codi personal amb ningú** i, encara menys, amb serveis tècnics desconeguts.

La dark web és la xarxa accessible mitjançant un programari específic i que, per les seves característiques d'anonimat i difícil traçabilitat, allotja multitud de mercats il·legals o continguts inadequats. Sovint el terme deep web s'utilitza com a sinònim, però, en realitat, es refereix a la part de la xarxa no visible per cercadors d'Internet (no indexada). La dark web és un subconjunt de la deep web.

Il·lustració 25. Tècnica utilitzada per al robatori del compte d'usuari a una xarxa social, en aquest cas Whatsapp[75, 76]

S'entén com hacktivisme *l'ús no violent d'eines digitals il·legals o legalment ambigües perseguint fins polítics.* Hacktivisme *és la fusió del* hackeig *i l'activisme, la unió de la tecnologia amb les intencions dels activistes.*

En bona part dels incidents, els ciberatacants tenen **motivacions *hacktivistes***, com els casos de segrest de comptes amb l'objectiu de difondre missatges interessats per ridiculitzar o cercar confrontació.

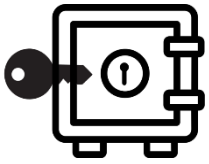
Per sobre de tot, els ciberatacants uilitzen la usurpació d'identitats per obtenir un benefici econòmic. És el cas del **segrest de comptes d'*influencers* amb l'objectiu de demanar un rescat a canvi de retornar-los-els**, ja que l'usuari legítim ho té força complicat per recuperar el control del compte. Segons constata una *instagrammer* lleidatana a qui han segrestat el seu compte, Instagram i Facebook "et fan omplir molts formularis que no serveixen per a res"[77]. Una altra estratègia dels ciberdelinqüents és la **creació de comptes falsos a les xarxes socials usats per recaptar diners de forma fraudulenta**, com succeí al ministre de *Asuntos Exteriores, Unión Europea y Cooperación* en funcions, Josep Borrell[78].

En altres casos, la usurpació d'identitat, mitjançant **falses promocions o sorteigs, té l'objectiu de recopilar les dades personals** dels qui s'hi subscriguin.

Usurpació d'identitat amb motivació econòmica

Més enllà de la usurpació de la identitat a les xarxes socials, els ciberdelinqüents fan ús d'una gran varietat de possibilitats per obtenir beneficis econòmics a partir de les dades personals dels usuaris.

Ús de targetes de crèdit/dèbit. Quan els cibercriminals disposen del número de la targeta de crèdit de la víctima, poden utilitzar-la per **realitzar compres no consentides**. No és difícil trobar gran quantitat de números de targetes de crèdit robades a Internet.



Usurpació del compte bancari. Els estafadors utilitzen tècniques d'enginyeria social, com el *phishing*, o la distribució de *malware* de tipus troià bancari amb l'objectiu d'obtenir el número de compte bancari i el PIN de la víctima. Les víctimes d'aquests atacs poden patir greus conseqüències si els cibercriminals aconsegueixen **obtenir préstecs o realitzar transferències al seu favor**.

[75] *https://faq.whatsapp.com/es/26000244/?category=5245246*
[76] *https://www.xataka.com/seguridad/como-le-han-quitado-cuenta-whatsapp-a-albert-rivera-que-puedes-hacer-no-te-pase-a-ti*
[77] *https://www.segre.com/es/noticias/cultura/2019/09/26/hackean_instagram_una_leridana_con_000_seguidores_87622_1112.html*
[78] *https://www.elmundo.es/espana/2019/09/02/5d6d5339fdddff830d8b4645.html*

Creació de falsos comptes bancaris. En altres casos, si el ciberdelinqüent disposa de prou dades personals, crea un nou compte sota el nom de la víctima. En aquest àmbit destaca el **robatori d'identitat infantil: les víctimes no disposen d'antecedents de crèdit**, cosa que facilita l'obertura de **nous comptes, sol·licitar ajudes públiques, contractar préstecs** i molt més. És possible que el menor no sàpiga que el seu crèdit s'ha utilitzat per saldar el seu deute fins al moment de sol·licitar préstecs escolars o de cotxes[79].

Robatori de la identitat mèdica. El robatori de la identitat mèdica persegueix l'obtenció de serveis mèdics i pot passar desapercebuda fins que es rep una factura per uns serveis mèdics dels quals mai s'ha fet ús.

Obtenció de préstecs en línia. Sovint, **la contractació d'un préstec en línia** passa per un procés d'aprovació automatitzat que mira de ser el més àgil possible. Les llacunes en els procediments poden derivar en la concessió de préstecs a prestataris suplantats.

Cobrament d'impostos. El robatori d'identitat fiscal pot permetre que un atacant demani la devolució dels impostos abans que la víctima.

En alguns casos, els ciberdelinqüents aconsegueix els seus propòsits **sense disposar de dades personals completes d'un usuari**. Es tracta de fraus d'**identitat sintètica**, en els quals es **fusionen dades personals de ciutadans reals amb altres de falses** per obtenir comptes i targetes de crèdit, dispositius mòbils o subscripcions a serveis en línia.

La usurpació d'identitat té solució?

La usurpació d'identitat seguirà sent una activitat lucrativa pel cibercrim mentre sigui possible obtenir dades personals a Internet i que aquestes siguin suficients per perpetrar accions que permetin obtenir algun tipus de benefici. Per trencar aquesta dinàmica calen accions col·lectives des de diferents àmbits, algunes de les quals ja estan en marxa.

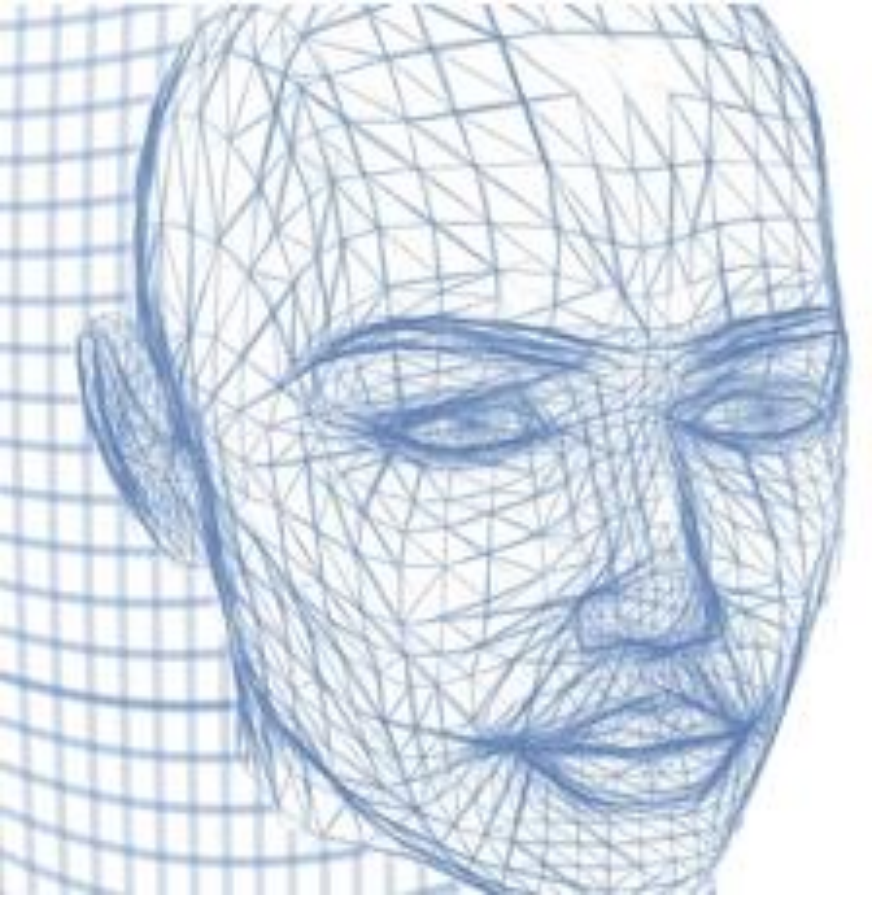
Els **responsables dels sistemes d'informació** han de **prendre mesures de ciberseguretat adequades per evitar les fuites d'informació**. En cas que no fossin suficients, **la informació i credencials emmagatzemades han d'estar xifrades**, de manera que els ciberdelinqüents no puguin fer-ne ús. Els **usuaris**, per la seva banda, han de **mantenir uns bons hàbits a la xarxa: utilitzar contrasenyes més complexes[80], evitar-ne la reutilització[81] i mantenir els equips actualitzats i protegits**. Ara bé, fins a dia d'avui, això no se segueix de forma suficient i calen mesures addicionals.

[79] *https://www.consumidor.ftc.gov/articulos/spdf-0010-robo-de-identidad-infantil.pdf*
[80] *https://internetsegura.cat/cybersecmonth-contrasenyes-segures/?doing_wp_cron=1578862363.0653200149536132812500*
[81] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/Informe-de-Tendencies-1er-trimestre-2019*

L'autenticació multifactor o de doble/triple factor és un tipus d'autenticació que es basa en un sistema de doble/triple clau, és a dir, un en què necessitaríem dos/tres elements per iniciar sessió. Elements relacionats amb: "una cosa que sabem", com una contrasenya, "alguna cosa que tenim", com un dispositiu mòbil, i/o "alguna cosa que som", com una empremta dactilar.

Des de les **autoritats reguladores**, també s'estan realitzant accions. La UE ha aprovat la **Directiva PSD2 (Payment Service Directive 2)**, la qual incideix en la ciberseguretat dels serveis de pagament amb l'objectiu de desenvolupar els sistemes en línia i mòbils, més segurs i una millor protecció del consumidor. Aquesta Directiva insta a utilitzar tecnologies d'autenticació multifactor per validar els pagaments electrònics: s'hauran d'acomplir simultàniament 2 o més dels 3 factors possibles i, com a mínim, un d'aquests factors no podrà ser ni reutilitzable ni reproduïble. A Espanya, **el 14 de setembre de 2019 la PSD2 va entrar en vigor, tot i que el Banc d'Espanya ha posposat *sine die*** (s'especula amb un termini d'un any) **l'aplicació de les mesures de seguretat de la norma a causa de la complexitat de la seva aplicació**[82]. Així, encara passaran alguns mesos abans no es pugui comprovar-ne els efectes positius.

A mig termini, també s'espera que irrompin les solucions tecnològiques d'**identitat sobirana** basades en ***blockchain*** La identitat sobirana, també anomenada **autosobirana, distribuïda o autogestionada**, permet que l'usuari disposi de les seves dades personals en propietat amb l'objectiu de controlar qui té accés a qualsevol informació sense necessitat de confiar en un dipòsit central de dades. La identitat sobirana no només permetrà millorar la privacitat de les dades, les quals estaran sota la custòdia de l'usuari, sinó que garantirà que ningú pugui fer-ne ús sense el seu consentiment i les protegirà de possibles fuites.



A Catalunya, el 7 de setembre la Generalitat de Catalunya va anunciar el **projecte IdentiCAT** per construir una **identitat digital descentralitzada i autosobirana**, **pionera a Europa i amb la qual es podran fer tota mena de tràmits en línia amb la protecció i el control de les pròpies dades**: "en qualsevol relació digital, el ciutadà podrà demostrar qualsevol atribut requerit de la seva identitat mantenint en tot moment la privacitat sobre la resta de dades contingudes en la seva ID"[83].

[82] *https://www.invertia.com/es/noticias/mis-finanzas/20190911/el-banco-de-espana-pospone-sin-fecha-la-nueva-norma-de-seguridad-en-pagos-electronicos-298036*
[83] *http://politiquesdigitals.gencat.cat/ca/detalls/Noticia/En-2-Minuts-IdentiCAT-el-nou-model-didentitat-digital-autosobirana-de-Catalunya*

Fets rellevants

- El CEO de Twitter va patir el *hackeig* del seu compte de la mateixa xarxa social, el qual va ser utilitzat per difondre missatges d'odi. Sembla ser que va ser originat a partir de la suplantació de la seva línia de telèfon[84].

- Aquest juliol el compte de Twitter de l'actriu **Jessica Alba** va ser *hackejat* per enviar **piulades intolerants, racistes i homofòbiques**[85].

- **Claude Béland**, antic president de Desjardins Group, la federació de cooperatives de crèdit més gran del Canadà, va denunciar haver estat **víctima de suplantació d'identitat** per a la sol·licitud de crèdits. **La federació va patir una fuita** quan un empleat va robar dades de **2,7 milions de persones** amb "finalitats malaltisses"[86].

- El juliol, els comptes de Twitter dels **ajuntaments de Pamplona, València i Albacete** van ser *hackejats* per **emetre missatges falsos**[87]

- Aquest setembre, **el departament de trànsit d'Arizona (EUA)** va anunciar **noves mesures de ciberseguretat** després de reconèixer que **164 conductors van ser objecte de robatori d'identitat i que les seves dades fossin utilitzades per crear comptes bancaris**[88].

- **Tots els Australians van ser instats a revisar els seus comptes de jubilació** després que es destapés un cas de frau d'identitat en què **es van obrir comptes bancaris a nom de multitud d'australians per a traspassar-hi diners dels comptes de jubilació i** usar aquests diners per a comprar actius, com joies i altres, per revendre'ls i tornar-los a Austràlia en forma de criptomonedes[89].

- **Un assistent de quiròfan** va ser detingut a Califòrnia (EUA) sota l'acusació de **robar les identitats i dades** financeres **de personal i personal del hospital on treballava** i utilitzar-les, per exemple, per a la **signatura de lloguer d'un pis**[90].
- Aquest setembre, **l'AEAT** (Agència Estatal d'Administració Tributària) va frenar diversos intents de *phishing* per missatges de correu i text que pretenien obtenir les **dades personals i bancàries dels ciutadans** que haguessin obert la porta a la usurpació d'identitat amb finalitats clarament econòmiques[91].

- **Segresten el compte d'Instagram d'una *influencer* lleidatana amb 27.000 seguidors** amb l'objectiu de demanar un rescat a canvi de retornar-li, així que ha hagut de crear-ne un de nou[92].

- El **compte de Twitter** del **president del València CF**, Anil Murthy, fou *hackejat* i va ser utilitzat per **publicar missatges d'odi**[93]

- El **compte d'Instagram de l'actor estatunidenc Jason Momoa**, amb més de **13 milions de seguidors**, va ser *hackejat*. Els ciberatacants publicaven imatges en què s'**anunciaven productes tecnològics de regal**, però en realitat només era un **mecanisme per recollir les dades personals**[94].

- L'**Albert Ribera**, líder del partit polític Ciutadans, va denunciar la usurpació del seu **compte de Whatsapp**, a partir de la qual els atacants van poder aconseguir la informació dels **xats i la valuosa agenda de contactes del polític**[95].

[84] *https://www.securityweek.com/twitter-ceo-account-hacked-offensive-tweets-posted*
[85] *https://www.scmagazine.com/home/security-news/data-breach/someone-hacked-the-twitter-account-of-actress-and-businesswoman-jessica-alba-to-post-bigoted-racist-and-homophobic-tweets-this-past-sunday/*
[86] *https://www.cbc.ca/news/canada/montreal/desjardins-former-president-identity-theft-data-breach-1.5210717*
[87] *https://ohmygeek.net/2019/08/20/robo-cuentas-twitter-agosto-2019/*
[88] *https://www.securityweek.com/drivers-license-thefts-spur-adot-boost-online-safeguards*
[89] *https://www.dailymail.co.uk/news/article-7472393/Jasmine-Vella-Arpaci-charged-online-fraud-scam-conned-victims-millions-dollars.html*
[90] *https://www.nbclosangeles.com/news/local/Surgical-Assistant-Suspected-of-Identity-Theft-Scheme-at-Southern-California-Hospitals-560084581.html*
[91] *https://www.lavanguardia.com/vida/20190917/47429924369/la-aeat-frena-intentos-de-fraude-con-mensajes-que-suplantaban-su-imagen.html*
[92] *https://www.segre.com/es/noticias/cultura/2019/09/26/hackean_instagram_una_leridana_con_000_seguidores_87622_1112.html*
[93] *https://eldesmarque.com/valencia/valencia-cf/noticias/209930-hackean-la-cuenta-de-anil-murthy-en-twitter-2*
[94] *https://www.elmundo.es/tecnologia/trucos/2019/09/05/5d7001c2fdddff66218b45de.html*
[95] *https://www.xatakamovil.com/seguridad/hackeo-whatsapp-albert-rivera-caso-suplantacion-identidad-muy-facil-evitar*


Baròmetre

Baròmetre

Top 5 ciberamenaces

Tenint en compte el nombre d'incidents que han tingut lloc durant el tercer trimestre de 2019, a continuació es mostra l'evolució de les cinc ciberamenaces més rellevants i se'n destaquen els esdeveniments més significatius.

Una ciberamenaça és qualsevol circumstància o esdeveniment que tingui un impacte potencial negatiu en alguna de les dimensions d'un actiu d'informació: confidencialitat, integritat i/o disponibilitat.

T3 2019	vs	T2 2019	Ciberamenaces[96]
1	=	1	**Compromís i/o pèrdua d'informació** Publicació d'informació o de credencials d'accés als sistemes d'informació de l'organització que la posen en compromís, així com informació de l'organització extraviada que no és recuperable de cap manera.
2	=	2	**Atacs deliberats** Difusió i/o execució de programari maliciós, accés lògic o físic no autoritzat, o abús de privilegis d'accés sobre els sistemes d'informació.
3	=	3	**Saturació i/o pèrdua de serveis essencials** Impossibilitat d'accedir als sistemes per inhabilitació o perquè han arribat a la màxima capacitat de processament, de manera que s'impedeix el correcte funcionament o es provoca l'aturada dels sistemes informàtics de l'organització.
4	=	4	**Coacció, extorsió o corrupció** Persuasió il·legítima, intimidació o suborn per obligar una víctima a cometre accions il·lícites o delictives contra els actius d'informació.
5	▲	6	**Informació errònia o corrupta (Integritat)** Informació errònia o corrupta de l'organització implicant que el contingut lògic d'aquests estigui organitzat d'una manera no apropiada, faltin dades o no sigui vàlid.

▲ Puja ▼ Baixa = Es manté

[96] *Catàleg d'amenaces de l'Agència de Ciberseguretat de Catalunya*

1. Compromís i/o pèrdua d'informació

Un servidor PACS és un sistema per emmagatzemar imatges radiològiques que s'utilitza principalment a entitats del sector sanitari.

Els logs són enregistraments seqüencials de tots els esdeveniments que afecten a un procés particular, de manera que conforma una evidència del comportament del sistema.

El compromís i/o pèrdua d'informació es manté com l'amenaça més habitual en el món de la ciberseguretat. **Només aquest trimestre s'han exposat més de 5.000 milions de registres**, entre les quals destaquen els casos de bases de dades del núvol obertes a causa d'errors de configuració. Així mateix, destaquen els incidents originats per **atacs dirigits als proveïdors de servei quan disposen de menys recursos en seguretat**.

- A final de juliol el **fabricant de software educatiu Pearson** (Regne Unit) va notificar una fuita de dades que afectava **les dades personals de 13.000 alumnes**, usuaris del software AIMSweb 1.0, de diferents escoles i universitats dels EUA. Segons indiquen, van poder resoldre la vulnerabilitat que havia causat l'incident, tot i que **les dades van estar exposades durant mesos**[97].

- A mitjan setembre, la companyia d'anàlisi i gestió de vulnerabilitats **Greenbone Networks** (Alemanya) va publicar un informe on es **destacava com 590 servidors PACS**, utilitzats al sector sanitari per la **gestió d'imatges radiològiques**, **exposaven públicament les dades personals dels pacients sense cap mena de protecció**. El mateix informe destaca un servidor a **Espanya amb 52.986 imatges exposades**[98].

- El proveïdor xinès de solucions **Smart Home Orvibo** va exposar **2.000 milions de *logs* d'usuaris a nivell global que contenien dades personals i contrasenyes** a causa d'un **servidor Elasticsearch mal configurat** sense usuari-password. Un dia després de fer-se públic, Orvibo va implementar una sèrie de mesures per protegir les dades dels usuaris[99].

- Una de les companyies bancàries més importants dels EUA, **Capital One**, va notificar que les dades personals i financeres de **106 milions de clients** que van sol·licitar targetes de crèdit entre 2005 i 2019 van ser compromeses després que un actor maliciós accedís als servidors aprofitant un **firewall mal configurat**[100].

- A mitjan setembre es va fer públic com les dades de **20 milions de ciutadans equatorians**, incloent-hi **7 milions de nens i persones ja mortes**, quedaven exposades públicament degut a un **servidor Elasticsearch mal configurat per un antic proveïdor de l'anterior govern**[101].

- Una **cadena espanyola de prostíbuls** va exposar dades extremadament sensibles, amb els **perfils complets de 3.350 noies**, com el nom, nacionalitat o fins i tot comentaris dels gerents, en una base de dades **MongoDB oberta públicament**. La base de dades també contenia dades dels clients, com el correu electrònic, els comentaris i les característiques dels seus dispositius[102].

[97] *https://www.pearson.com/corporate/news/media/news-announcements/2019/07/pearson-customer-notification.html*
[98] *https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf*
[99] *https://www.bleepingcomputer.com/news/security/billions-of-records-including-passwords-leaked-by-smart-home-vendor/*
[100] *https://www.cnbc.com/2019/07/30/capital-one-hack-allegations-describe-a-rare-insider-threat-case.html*
[101] *https://securityaffairs.co/wordpress/91337/data-breach/ecuador-data-leak.html*
[102] *https://gdpr.report/news/2019/08/12/database-belonging-to-spanish-brothel-chain-exposed/*

2. Atacs deliberats

Un troià d'accés remot o RAT és un programari maliciós que infecta la víctima fent-se passar per un programari lícit i que estableix una connexió amb el hacker *donant-li control sobre el dispositiu de la víctima.*

Una plataforma de canvi de criptomonedes és la plataforma web des de la qual és possible comprar i vendre criptomonedes a canvi de contraprestacions econòmiques, en concepte de monedes de curs legal o d'altres criptomonedes.

*Una APT (*Advanced Persistent Threat*) o Amenaça Persistent Avançada és un atac format per un conjunt de processos informàtics sigil·losos, continuats i que fan ús de múltiples vectors d'atac, dirigits a penetrar la seguretat informàtica d'una* entitat específica.

Els atacs deliberats continuen en segona posició. Aquest trimestre, els atacs dirigits amb *ransomware* han estat els principals protagonistes (veure capítols Botnets i Ransomware dirigit) però no han estat els únics.

- Un informe de Trendmicro del juliol exposa una nova **campanya de correu brossa**, dirigida a Sud-amèrica, per instal·lar un troià d'accés remot anomenat "**Project RAT".** Segons indiquen, **l'objectiu de la campanya són entitats governamentals o institucions sanitàries**, entre d'altres[103].

- A mitjan juliol, la plataforma de canvi japonesa **Bitpoint** va haver d'**aturar la seva activitat** després de la detecció d'un **error en el sistema de transmissió de fons a causa de l'accés no autoritzat d'un actor maliciós**. L'empresa va perdre fins a **32 milions de dòlars**[104].

- A final de juliol, les **empreses alemanyes BASF, Siemens i Henkel van ser atacades per un grup de ciberespionatge** que es vincula amb la **Xina** a causa de les tècniques APT utilitzades. La campanya també va afectar altres empreses en l'àmbit mundial com el gegant farmacèutic Roche[105].

- A l'agost, l'empresa de ciberseguretat **Group-IB** va prevenir una **campanya** de falsa publicitat a les **xarxes socials dirigida a consumidors de llengua espanyola i italiana** amb l'objectiu de robar-los dades o subscriure'ls a serveis de pagament. S'utilitzaven marques conegudes com **Alitalia o Carrefour,** entre d'altres[106].

- Investigadors de Palo Alto van publicar la detecció de la **campanya de troians** dirigits contra **companyies navals i de transport** del **Golf Pèrsic.** Les eines anomenades **xHunt**, per les referències a una sèrie d'*anime* van ser detectades a partir d'una empresa infectada i inclouen funcionalitats avançades per passar desapercebudes i controlar totalment l'equip de la víctima[107].

- A mitjan setembre la companyia **Thinkful**, dedicada a la formació de programació en línia, va informar als seus clients de l'**accés no autoritzat a les seves credencials** i que procedia a restablir tots els comptes. A causa de la falta d'informació, **s'especula que un empleat fos víctima de *phishing*** i filtrés el seu usuari i contrasenya[108].

[103] *https://gbhackers.com/proyecto-rat-uses-email-service/*
[104] *https://www.infosecurity-magazine.com/news/japanese-exchange-bitpoint/*
[105] *https://securityaffairs.co/wordpress/88900/breaking-news/basf-siemens-henkel-cyber-attacks.html*
[106] *https://securityaffairs.co/wordpress/89287/cyber-crime/lotsy-group-scam-campaigns.html*
[107] *https://www.zdnet.com/article/hackers-target-transportation-and-shipping-industries-in-new-trojan-malware-campaign/*
[108] *https://www.bleepingcomputer.com/news/security/thinkful-resets-all-user-passwords-after-security-breach/*

3. Saturació i/o pèrdua de serveis essencials

Els atacs DDoS i *ransomware* han estat protagonistes dels incidents que han causat aturades de l'activitat productiva durant aquest trimestre.

- **Imperva** va detectar el que sembla ser l'atac DDoS més gran de la historia fent ús de peticions d'aplicació (Capa 7 del model OSI[109]).

- A principi de juliol, **Cloudflare va patir interrupcions de servei que van afectar aplicacions** com Discord i Feedly entre d'altres després d'implementar noves regles al seu Firewall que tenien l'objectiu de prendre mesures per protegir als seus clients[110].

- A l'agost, **el centre mèdic rural Wood Ranch Medical** (EUA) es va veure afectat per un atac de *ransomware* que va afectar la informació de 5.835 pacients i va arribar a xifrar les còpies de seguretat. Es desconeix si es va realitzar el pagament del rescat, però en qualsevol cas la informació va resultar irrecuperable i va obligar al **cessament permanent de l'activitat del centre** [111].

- A principi de setembre, una de les empreses més grans d'audiòfons, **Demant**, va patir un atac que **va obligar a tancar tota la seva infraestructura informàtica**. L'incident va fer que tinguessin **problemes en la recepció i subministrament de comandes** que pot haver causat pèrdues **d'aproximadament 95 milions de dòlars**[112].

- El darrer setembre, **Wikipedia** va patir un atac **DDoS** que va durar 3 dies. Tot i disposar de **mesures anti-DDoS**, no es va poder evitar que **Wikipedia perdés la disponibilitat en el 40% dels seus servidors** i va afectar el servei als usuaris d'**Europa** i **Orient Mitjà**, principalment[113].

- Durant el cap de setmana del 21 de setembre, **un proveïdor de serveis d'internet de Sud-àfrica va patir un atac DDoS** que va provocar la **pèrdua intermitent de connectivitat** a Internet dels seus clients, així com una velocitat de connexió més lenta[114].

- A final de setembre, el proveïdor de serveis de defensa i fabricant de parts de cotxes **Rheinmetall va haver d'aturar la producció a les seves plantes als EUA, Brasil i Mèxic a causa d'un atac amb *malware***. L'empresa no va especificar quin tipus de *malware* va causar la disrupció[115].

[109] *https://en.wikipedia.org/wiki/OSI_model*
[110] *https://www.elespanol.com/omicrono/20190704/simple-linea-escrita-perdieses-acceso-favoritas-semana/411210022_0.html*
[111] *https://www.hipaajournal.com/wood-ranch-medical-announces-permanent-closure-due-to-ransomware-attack/*
[112] *https://www.newnettechnologies.com/hearing-aid-giant-demant-warns-of-extreme-losses-due-to-ransomware-attack.html*
[113] *https://nakedsecurity.sophos.com/2019/09/11/wikipedia-fights-off-huge-ddos-attack/*
[114] *https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/#ftag=RSSbaffb68*
[115] *https://www.securityweek.com/german-auto-and-defense-firm-rheinmetall-says-malware-hit-several-plants*

4. Coacció, extorsió i/o corrupció

La sextorsió o sextortion *és una forma d'explotació sexual en el qual es fa xantatge a una persona amb una imatge o vídeo sexual seu, en què apareix despullat o realitzant actes sexuals, que generalment ha estat compartit prèviament mitjançant* sexting.

Ja s'ha vist repetidament com el *ransomware* ha estat un dels atacs més destacats del trimestre i una de les seves característiques principals és l'extorsió a les seves víctimes. **Cada cop s'utilitzen més tècniques per pressionar la víctima amb l'objectiu que pagui el rescat de manera immediata** com, per exemple, esborrant arxius o incrementant el preu del rescat cada cert temps (veure capítol *Ransomware dirigit*).

Els casos de *sextorsió* també segueixen una tendència a l'alça. Segons informa Symantec, durant els **5 primers mesos de l'any ha bloquejat 300 milions de correus d'extorsió**[116].

- A principi de juliol l'**FBI**n va alertar d'una **campanya de *sextorsió* dirigida a adolescents**. Segons indiquen, alguns joves es van veure tan afectats que van **plantejar-se el suïcidi per escapar de la situació**. L'FBI va alertar que els afectats tenien entre **10 i 17 anys i que la majoria dels casos comencen des de plataformes de jocs**[117].

- A mitjan juliol, la base de dades de l'editorial mexicana **Librería Porrúa** va exposar **1,2 milions de registres** a causa d'una instància de **MongoDB sense cap mena de protecció**. Es dona el cas que la base de dades mal configurada va ser primerament detectada per un investigador però, atès que la companyia no va actuar, tres dies després **un *hacker* va esborrar les dades** i va demanar un **rescat de 500 dòlars** a canvi de recuperar-les[118].

- Eset va publicar un nou informe sobre la detecció d'un *malware* anomenat **Varenyky** de tipus *botnet*. Els equips infectats envien diferents tipus de **correu brossa** pel port SMTP **dirigits a usuaris francesos**. Els fitxers adjunts són maliciosos, per seguir propagant la *botnet*, i en alguns casos remeten a **portals de *phishing*** i en altres **amenacen de publicar un vídeo sexual** de la víctima si no es paguen **750 €**[119].

- A final d'agost, es va detectar una **campanya de *sextorsió*** promoguda pel grup de hackers ChaosCC, en la qual s'amenaçava els usuaris amb la difusió de vídeos enregistrats des de la càmera web mentre estaven mirant pàgines per adults si no es feia el pagament de **700 dòlars en bitcoin**[120].

- Al setembre, es va advertir d'una **campanya de *sextorsió*** que es duia a terme a **Irlanda**. El correu electrònic **acusava les víctimes de ser pedòfils** i els advertia que **havien estat gravats** i demanaven **una quantitat econòmica a canvi de no exposar a la família i coneguts els seus secrets**[121].

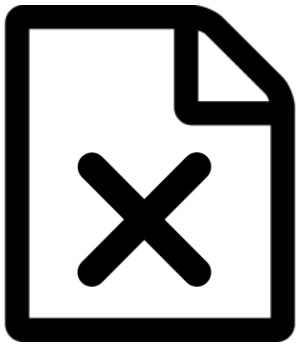
[116] *https://www.symantec.com/blogs/threat-intelligence/email-extortion-scams*
[117] *https://securityaffairs.co/wordpress/87996/cyber-crime/fbi-warns-sextortion-teenagers.html*
[118] *https://www.bleepingcomputer.com/news/security/ransom-note-replaces-21m-customer-records-on-open-mongodb/*
[119] *https://www.welivesecurity.com/2019/08/08/varenyky-spambot-campaigns-france/*
[120] *https://www.bleepingcomputer.com/news/security/latest-sextortion-email-scheme-sent-by-chaoscc-hacker-group/*
[121] *https://www.infosecurity-magazine.com/news/ireland-hit-by-pedophile*

5. Informació errònia o corrupta (integritat)

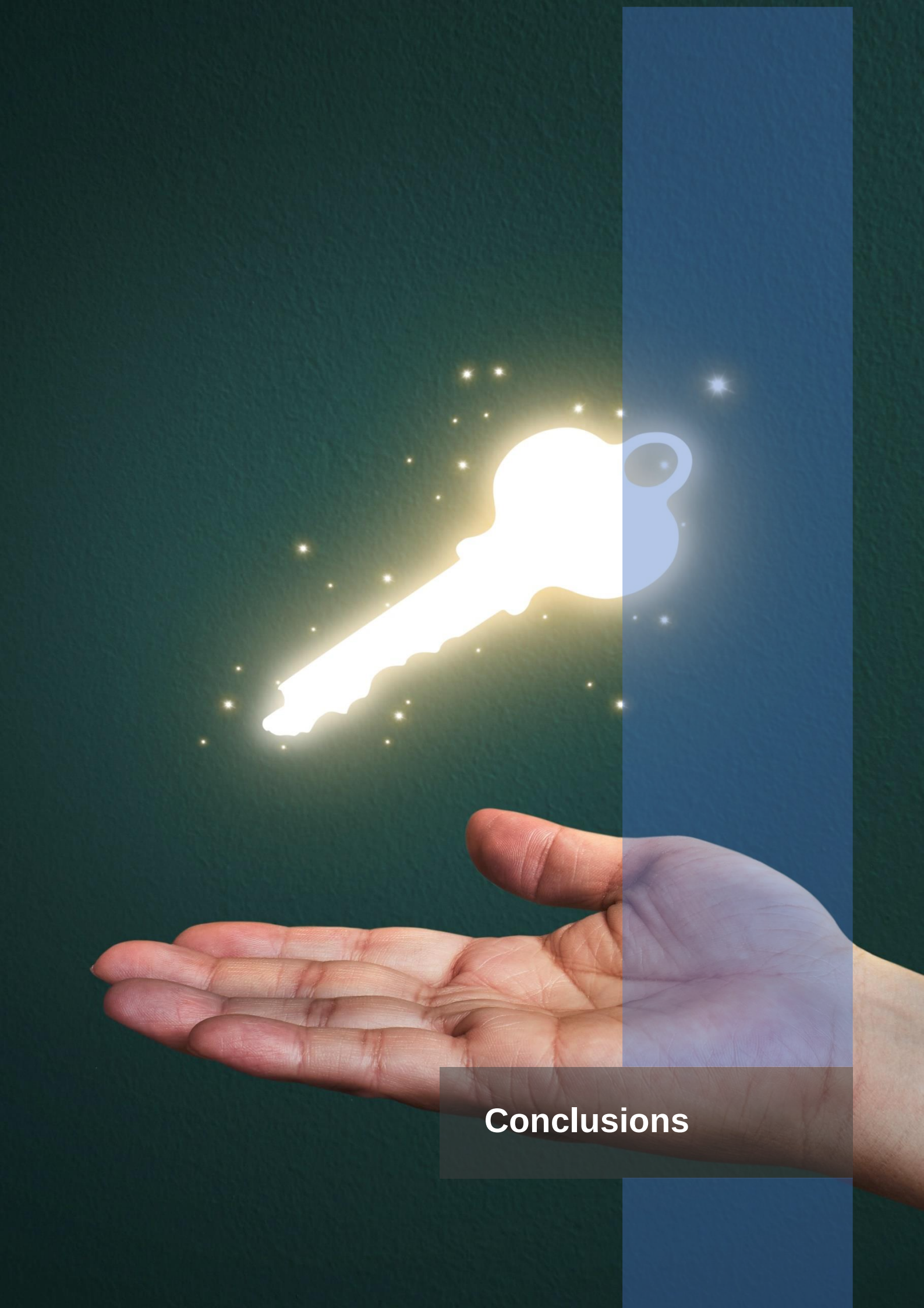
Un wiper és un programari maliciós que té la intenció de destruir sistemes i/o dades amb la intenció de generar danys a la víctima.

L'amenaça d'informació errònia o corrupta pren força a causa de l'increment d'atacs de *ransomware* dirigit. Cal destacar com també és cada cop és més habitual **l'ús de *wipers* o elements destructius**, com indica un informe d'IBM que alerta d'un **creixement de *malware* destructiu del 200% durant la primera meitat del 2019**[122].

- Segons **The New York Times**, al mes de juny, **Iran va patir un atac dels EUA** en el qual es van **esborrar equips i bases de dades** que suposadament s'utilitzaven per planificar atacs contra vaixells de tancs de petroli. Segons indiquen, l'atac va ser la **resposta a l'enderrocament d'un *drone* estatunidenc**[123].
- A mitjan juliol, un grup de *hackers* va atacar el **centre de desenvolupament d'Hongria i va destruir les seves bases de dades digital** que contenien dades oficials i contractes[124].
- A final de juliol es va detectar una campanya de difusió del ***wiper* GermanWiper**, el qual **reescriu tots els arxius amb zeros**. Posteriorment, demana un rescat a l'afectat tot i que **les dades són irrecuperables**[125].
- També a Alemanya, durant el mes de setembre, va començar una **campanya de correu brossa** que, amb un currículum i fotografia en PDF adjunts, amagava un executable **que** instal·lava el *wiper* **Ordinypt** i **destruïa els arxius de la víctima**. Els atacants **demanaven rescat tot i que els arxius no eren recuperables**[126].



[122] *https://arstechnica.com/information-technology/2019/08/ransomware-wiper-malware-attacks-have-more-than-doubled-ibm-team-says/*
[123] *https://oilprice.com/Energy/Energy-General/New-York-Times-US-Hacked-Iran-To-Prevent-Oil-Tanker-Attacks.htmlmi*
[124] *https://www.ibtimes.sg/hacker-destroys-hungarian-development-centers-digital-database-32408*
[125] *https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/*
[126] *https://www.bleepingcomputer.com/news/security/destructive-ordinypt-malware-hitting-germany-in-new-spam-campaign/*



Conclusions

Conclusions

El 1986 aparegué **Brain, el primer virus dirigit contra la plataforma PC d'IBM** (i, per extensió, al sistema operatiu MS-DOS) i el primer d'utilitzar tècniques d'ocultació. En poques setmanes va propagar-se arreu del món a través de discs *floppy*. Dos anys més tard aparegué **el primer cuc, Morris**, que es va propagar per milers d'ordinadors de la xarxa, aleshores encara ARPAnet[127]. Es dona el cas que cap dels *malwares* inicials va ser creat per ser maliciós ni per propagar-se tant ràpidament[128].

Han passat més de 30 anys i els *malwares* han evolucionat molt, de la mà de l'evolució tecnològica i d'uns usuais cada cop més experts, i han anat incorporant noves capacitats. Així, han sorgit programaris maliciosos especialitzats de tipus **virus, cuc, troià, *botnet*, *keyloggers*, RAT, *rootkit*, etc**.

Avui dia, els programaris maliciosos s'han convertit en una eina que obre les possibilitats d'un **autèntic negoci pel cibercrim**, cosa que ha suposat l'impuls definitiu. La motivació econòmica és cabdal per entendre com els *malwares* han evolucionat i s'han convertit en **eines complexes, polivalents i contínuament canviants**. La recent onada d'atacs realitzats pel *malware* **Emotet** n'és un exemple i això es constata quan es tracta de classificar-lo d'acord amb les seves funcionalitats: **troià-*keylogger*-*botnet*-*spyware*-*dropper*...** Així mateix, aquests atacs amaguen l'autoria combinada de diversos operadors criminals, cada un especialitzat en la seva àrea d'expertesa.

Per a més inri, aquests programaris maliciosos s'escampen mitjançant **avançades tècniques d'enginyeria social** que exploten la confiança de les víctimes, cosa que els fa encara més perillosos; fins al punt que, actualment, un correu electrònic des d'un remitent de confiança no és cap garantia de seguretat! L'explotació del **factor humà** realça, encara més, el potencial de l'amenaça.

L'escenari existent i futur és desafiant, però de la mateixa manera que els *malwares* Brain i Morris van tenir una resposta adequada i es van poder mitigar, **els nous i avançats programaris maliciosos també tindran la corresponent contrarèplica amb l'aparició d'eines de ciberseguretat intel·ligents**. L'aposta per la IA en ciberseguretat ja no és una elecció, sinó que esdevé imprescindible.

[127] *https://www.welivesecurity.com/la-es/2016/10/24/historia-del-malware-actualizada/*
[128] *https://www.welivesecurity.com/2018/11/05/malware-1980s-brain-virus-morris-worm/*

Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

ciberseguretat.gencat.cat