Universitat Autònoma de Barcelona

Millorant les ciber assegurances: Una reflexió sobre la protecció digital en el món empresarial.

Autor: Vladyslav Katerynchuk Serrano (1567511)
Tutor: Genis Margarit Contel

Treball de Fi de Grau

Grau d'Empresa i Tecnologia

Universitat Autònoma de Barcelona

30 de maig del 2023

Agraïments

Primerament, m'agradaria agrair al meu tutor Genis Margarit Contel pel seu treball durant la realització d'aquest TFG, perquè m'ha guiat de com fer el TFG i ser nexe de contacte amb la Maria Torra Badia, contacte rellevant per l'elaboració del punt més important del treball. Finalment, vull agrair a Maria Torra Badia, CEO de Dracma, i a Felipe López Pinto, Propietari de Verbien, per a la seva col·laboració en el meu treball, sense ells el punt de les assegurances no hauria sigut el mateix.

Resum

Durant aquest treball es tractaran diversos temes, els quals tenen a veure amb la ciberseguretat, tema molt important avui dia perquè cada cop els cibercriminals i ciberdelinqüents són més una organització criminal organitzada, la qual es lucra amb activitats il·lícites. Les tecnologies avancen i no només per a les empreses i entitats governamentals, sinó que per aquests grups criminals també, punt importat a tenir en compte perquè cada vegada tenen eines més potents per fer les seves activitats.

En el treball es tractarà la situació actual de la ciberseguretat, tant en l'àmbit nacional com internacional, també es farà un enfocament a un servei nou ofert pels grups criminals, el qual és el RaaS (Ransomware as a Service) i s'intentarà accedir a un d'aquests serveis a la "Dark Web" per mostrar el fàcil que és ser un ciberdelinqüent avui dia. Finalment, es tractarà la part principal d'aquest treball, la qual tracta les ciber assegurances, perquè són un producte que pot ser crucial per a les empreses avui dia i com es podria millorar la venda d'aquests, ja que no és un producte molt conegut. Aquesta part final es tractarà amb l'ajuda de dues col·laboracions i són la CEO d'una empresa d'assegurances, la qual tracta les ciber assegurances, seguidament amb la col·laboració del propietari d'una PIME, per així veure el seu punt de vista sobre les ciber assegurances i també de les seves experiències amb incidents.

Paraules clau

Ciberseguretat, RaaS, Ciberassegurances i *Dark Web*

Índex

Taula de continguts

1. Què és la seguretat de la informació?

En aquest punt del meu treball de final de grau, m'enfocaré a analitzar i comprendre els aspectes fonamentals de la seguretat de la informació. Començaré examinant la importància del Big Data en el món actual i entenent la diferència entre les dades i la informació. A més, destacaré la importància de protegir aquestes dades i informació a causa de la quantitat d'informació confidencial i valuosa que manegem avui dia. És crucial comprendre aquests conceptes per a tenir una visió clara de la situació actual de la ciberseguretat i els desafiaments que enfronten les empreses.

La seguretat de la informació té diverses definicions, però segons el meu criteri al dia d'avui la definició donada per IBM exposa molt bé el que és la seguretat de la informació i és la següent:

"La seguretat de les dades és la pràctica que consisteix a protegir la informació digital contra l'accés no autoritzat, la corrupció o el robatori durant tot el seu cicle de vida. És un concepte que comprèn tots els aspectes de la seguretat de la informació, des de la seguretat física del maquinari i els dispositius d'emmagatzematge fins als controls administratius i d'accés, així com la seguretat lògica de les aplicacions de programari. També inclou les polítiques i els procediments de l'organització." [1]

Microsoft té una bona definició també, però la mencionada anteriorment d'IBM acaba d'exposar més parts que formen part de la seguretat de la informació. La definició és la següent:

"La seguretat de la informació, que sol abreujar-se com InfoSec, és un conjunt de procediments i eines de seguretat que protegeixen àmpliament la informació confidencial de l'empresa enfront de l'ús indegut, accés no autoritzat, interrupció o destrucció. InfoSec comprèn la seguretat física i de l'entorn, el control d'accés i la ciberseguretat. Sol incloure tecnologies com a agent de seguretat d'accés al núvol (CASB), eines d'engany, detecció i resposta en el punt de connexió (EDR) i proves de seguretat per a DevOps (DevSecOps), entre altres." [2]

Ens podem fixar que ambdues de les definicions parlen de la seguretat de la informació, però la d'IBM comença parlant sobre la seguretat de les dades, el qual és interessant perquè les dades no és el mateix que la informació, diferència rellevant, ja que la informació té més contingut sensible que les mateixes dades, sobretot per a les empreses que construeixen una estratègia sobre l'anàlisi de dades.

1.1. La importància del Big Data avui dia i la diferència entre informació i dades

Per què és important el Big Data avui dia per a les empreses? El Big Data permet a les empreses prendre decisions més informades, ja que els proporciona una gran quantitat d'informació sobre els seus clients, les seves operacions i el seu entorn. Per exemple, a través de l'anàlisi de dades, les empreses poden conèixer millor al seu públic objectiu, la qual cosa els permet personalitzar els seus missatges i ofertes per a atendre millor les seves necessitats. A més, també poden optimitzar les seves campanyes de màrqueting per a aconseguir un major impacte i una major eficiència en les seves despeses.

Es poden observar millores en el camp de la producció i dedicions estratègiques, gràcies al Big Data, perquè amb l'anàlisi de les dades (informació) es poden solucionar problemes d'eficiència en temps real (millorar productivitat i reduir costos), també per optimitzar processos. En la part de decisions estratègiques l'anàlisi de dades juga un paper important, ja que ajuda a les empreses identificar noves oportunitats de negoci, detectar patrons i tendències del mercat, la qual cosa ajuda molt a mantenir el seu avantatge competitiu.

Com exposa l'article sobre el Big Data la universitat UNIR també gràcies a aquest es poden determinar comportament fraudulent, ja no només és pel tema financer sinó que es pot utilitzar en l'àmbit de la ciberseguretat, com per exemple connexions inesperades dins d'una xarxa i detectar aquests patrons atípics per poder actuar degudament, ja que permet a les empreses i organitzacions recopilar i analitzar grans quantitats d'informació sobre la seva activitat en línia i l'activitat dels usuaris, la qual cosa els permet identificar patrons i tendències que suggereixin activitat malintencionada.[3]

A més a més, l'anàlisi de dades també pot utilitzar-se per a detectar i prevenir atacs cibernètics en temps real, la qual cosa els permet a les empreses i organitzacions protegir-se de possibles amenaces i mitigar els riscos de seguretat.

Com he mencionat anteriorment les dades no és el mateix que la informació, ja que la informació conté una anàlisi de les dades o informació delicada. Amb això no vull dir que la informació sigui sempre molt més important que les dades, perquè també poden haver-hi dades confidencials, com per exemple, les dades personals dels clients d'una empresa. Les dades són majoritàriament inputs que reben de diferents llocs, com podria ser els productes que es venen en el seu negoci, generant així moltes dades i emmagatzemar-les en un magatzem de dades (Data Warehouse). Però aquestes dades són això només dades, les quals després han de ser analitzades amb un equip d'analistes de dades i treure informació rellevant sobre aquestes dades, perquè si no es transformarien en dades fosques, és a dir, dades que només es tenen, però no es treuen valor sobre elles.

En aquest procés les empreses gasten una gran suma de diners, per poder crear estratègies sobre els anàlisis, per exemple, Netflix utilitza les seves dades per poder recomanar pel·lícules i sèries als seus usuaris, és a dir, utilitza tots els inputs que els hi proporcionen els usuaris, els quals després són utilitzats pel seu algorisme per poder recomanar el que segurament li agrada a l'usuari, perquè es quedi més temps a la plataforma. Un altre exemple semblant

podria ser Amazon, ja que posiciona productes que podrien ser més interessants pels clients. En el cas que alguna de les dues empreses, patis un ciberatac i filtressin els seus algorismes, per exemple, perdrien el seu avantatge competitiu perquè si aquesta informació arriba a altres empreses, es podrien copiar.

1.2. Importància de protegir la informació

La protecció de les nostres dades i informació és molt important, però no només s'ha de protegir sinó que s'ha d'analitzar realment que és el que s'ha de protegir i com, ja que no totes les empreses es poden permetre fer una inversió molt gran per protegir-ho tot. La protecció d'aquesta informació com he deixat intuir en el punt anterior és molt important per no influir directament a l'activitat de l'empresa, però hi ha més factors que poden ser perjudicats [4] i poden ser:

- **Propietat intel·lectual:** La informació confidencial de l'empresa, com podrien ser els seus productes, prototips, estratègies i patents, és valuosa i s'ha de protegir per evitar que aquesta sigui utilitzada indegudament per tercers.

- **Compliment legal:** A les empreses se li exigeix que compleixin unes normes en el cas de tractar dades delicades de clients. Necessiten acreditar-se amb un estàndard per a demostrar que les dades dels clients estan fora de perill amb ells. Aquest estàndard és l'ISO 20000 [5], el qual garanteix que els sistemes de gestió i suport de les tecnologies de la informació d'una empresa segueixen les millors pràctiques. Es revisen temes com els processos de serveis, relacions, resolucions i control. Amb l'adquisició d'aquest estàndard garanteixes que el client rebrà un servei de qualitat i que segueixes les millors pràctiques reconegudes en l'àmbit internacional.

- **Reputació:** La pèrdua o el robatori d'informació confidencial pot danyar la reputació d'una empresa i afectar la seva credibilitat en el mercat. Per aquest simple motiu, les empreses no denuncien els seus atacs, perquè els perjudica molt de cara als seus stakeholders. A Espanya les empreses incompleixen l'obligació genèrica de denunciar aquests cibercrims, perquè la multa és només de 250 pessetes [6] (1,5 €).

- **Pèrdues financeres:** Depenent de com s'ha actuat en el cas de patir un àtac, l'empresa pot patir pèrdues financeres. Per exemple, si una empresa de producció treballa sota demanda, en el cas de patir un atac que parés la producció pararien de guanyar diners, ocasionant moltes pèrdues. També haurien de gastar diners per recuperar-se, és a dir, millor invertir en mesures preventives.

- **Privacitat dels clients:** Es poden veure exposades dades confidencials dels clients, els quals també surten perjudicats amb les exposicions de dades. El client és un factor molt important de l'empresa i pot afectar directament al rendiment d'aquesta.

La protecció de la informació a una empresa afecta positivament a una sèrie de factors, com poden ser els següents:

- **Millorar la presa de decisions:** La informació confidencial i precisa és essencial per a prendre decisions informades i estratègiques en una empresa. Si la informació és compromesa o es perd, pot afectar la capacitat de l'empresa per a prendre decisions efectives.

- **Evitar sancions i multes:** La falta de protecció adequada de la informació pot resultar en sancions i multes per incompliment de lleis i regulacions, la qual cosa pot tenir un impacte negatiu en les finances de l'empresa.

- **Protecció d'actius crítics:** La informació crítica, com les claus de seguretat i els sistemes d'informació, ha de protegir-se per a evitar l'accés no autoritzat i per a mantenir la integritat dels actius crítics de l'empresa.

- **Mantenir la confiança dels inversors:** La protecció adequada de la informació confidencial és essencial per a mantenir la confiança dels inversors i per a atreure nous inversors.

En resum, protegir la informació, la propietat intel·lectual, actius crítics i complir amb les obligacions legals i ètiques d'una empresa, és crucial per garantir el seu èxit.

Com a exemple, l'empresa que va patir un ciberatac i va perjudicar la seva reputació tenim a Yahoo!, ja que va patir dos ciberatacs, un l'any 2013 i un altre el 2014, però no ho van revelar fins al 2016, en els quals van ser compromeses 1,5 mil milions de comptes de clients. Amb aquests atacs van perdre informació delicada, inclòs noms d'usuaris, contrasenyes, dates de naixement i adreces de correu electrònic. A més, els atacants també van obtenir accés a preguntes de seguretat i respostes que els usuaris havien configurat per a protegir els seus comptes.

L'impacte econòmic del ciberatac de Yahoo! va ser significatiu. La companyia va experimentar una disminució en el valor de les seves accions i una disminució en la confiança en el mercat. A més, Yahoo! va haver d'enfrontar-se a diverses demandes dels usuaris afectats pel ciberatac i va haver d'invertir en la millora de la seguretat dels seus sistemes. [7]

Aquest ciberatac és un exemple important de per què és necessari que les empreses inverteixin en mesures de seguretat cibernètica efectives. És essencial que les empreses protegeixin la informació confidencial dels seus usuaris i evitin els costosos impactes econòmics d'un ciberatac.

2. Situació actual de la ciberseguretat

En un món cada vegada més digital, la ciberseguretat és una preocupació clau per a les organitzacions i les nacions. Amb la creixent dependència de la tecnologia i la informació, és vital assegurar la seguretat dels sistemes i la informació confidencial. En l'àmbit global, la ciberseguretat és un tema cada vegada més important a causa de l'augment constant dels ciberatacs i la ciberdelinqüència.

A més, les empreses estan experimentant dificultats per a trobar talent capacitat en ciberseguretat, la qual cosa posa en risc la seguretat de la informació i els sistemes. La necessitat de professionals altament capacitats en ciberseguretat ha augmentat ràpidament, però l'oferta de professionals qualificats no ha augmentat al mateix ritme. Això ha portat a una escassetat de talent en ciberseguretat i a una competència feroç per part de les empreses per a atreure i retenir als millors professionals.

En aquest punt del treball, ens centrarem a examinar la situació actual de la ciberseguretat a escala global, així com la situació a Espanya. També explorarem els problemes que enfronten les empreses per a trobar talent en ciberseguretat i com estan abordant aquesta escassetat de talent per a poder combatre les noves amenaces en ciberseguretat.

2.1. Situació des d'una visió global

La situació actual en la ciberseguretat a nivell mundial és desafiadora i en constant evolució. A mesura que la tecnologia es torna més avançada i s'integra cada vegada més en les nostres vides, també augmenta l'exposició als ciberatacs i la necessitat de protegir-se contra ells.

A més, els ciberatacs estan en constant evolució i es tornen cada vegada més sofisticats, la qual cosa els fa més difícils de detectar i prevenir. Aquests ciberatacs poden tenir conseqüències greus en termes de privacitat, seguretat de dades i danys econòmics, i poden afectar empreses, organitzacions governamentals i persones a tot el món.

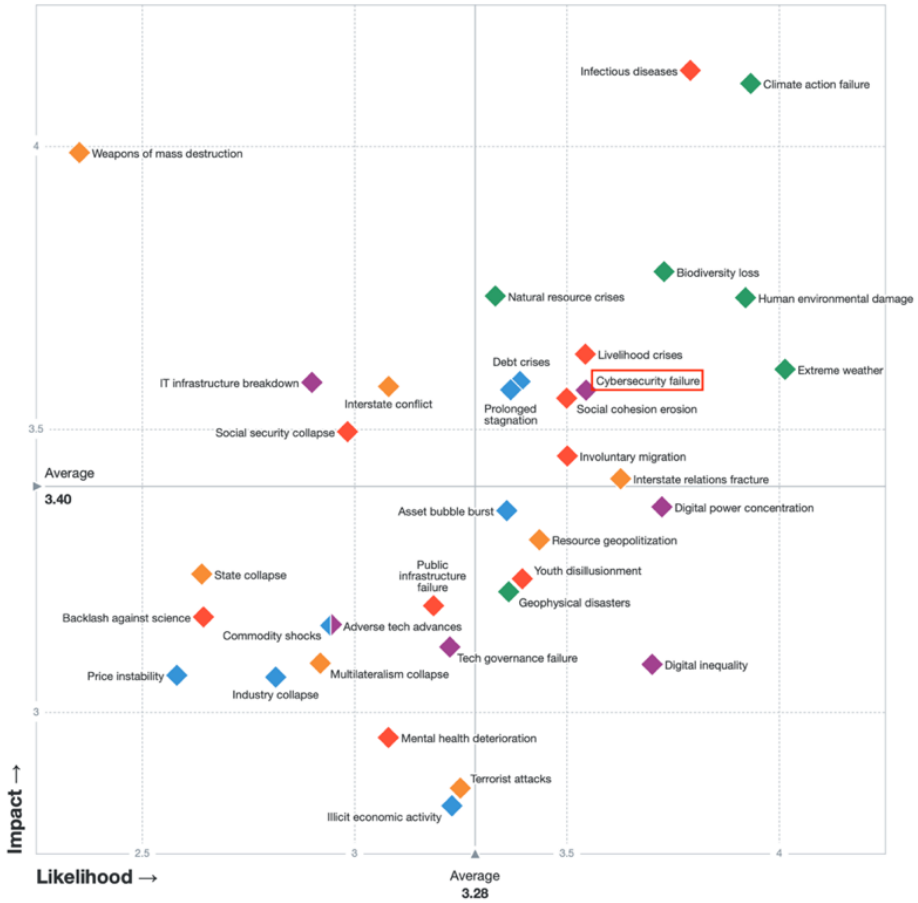
Malgrat els avanços en la tecnologia de seguretat cibernètica i la consciència global sobre la importància de la ciberseguretat, la tasca de protegir-se contra els ciberatacs continua sent un desafiament constant. És necessari un esforç continu i col·laboratiu internacionalment per a abordar aquests desafiaments i garantir una ciberseguretat adequada per a tots.[8]

Podem observar una clara preocupació sobre els ciberatacs, la qual està s'està incrementant any rere any. Podem analitzar que al *"The Global Risks Report 2021"*[9] una preocupació amb un impacte i probabilitat altes es troben les falles en ciberseguretat, és a dir, és una preocupació mundial real.

Els ciberatacs porten temps sent una preocupació mundial, es pot veure en el mateix report, però de l'any 2015[10] perquè estava situada gairebé a la mateixa posició, però des de l'any 2021 (Figura 1) la preocupació s'ha transformat lleugerament, perquè ja no és la preocupació que hi hagi ciberatacs, sinó que hi hagi falles de seguretat.

Figura 1

Situació de riscos globals 2021.



Nota. De The Global Risks Report 2021 (p.12), per McLennan, M., & Group, S., 2021, (https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf). En domini públic.

Personalment, crec que és més encertada aquesta preocupació, perquè els ciberatacs poden continuar existint, però no vol dir que acabin de tenir èxit.

Cada dia hi ha milions d'atacs arreu del món, com podem observar en la Figura 2. Aquesta imatge ha sigut extreta d'una pàgina web de l'empresa d'antivirus Kaspersky, la qual recopila en temps real els atacs que es detecten. En aquesta imatge es pot analitzar d'una manera visual els atacs que són produïts arreu del món, ja que es poden apreciar d'on surten els atacs i on van dirigits, donant a entendre que la situació amb els ciberatacs és un problema mundial.[11] [12]

Figura 2

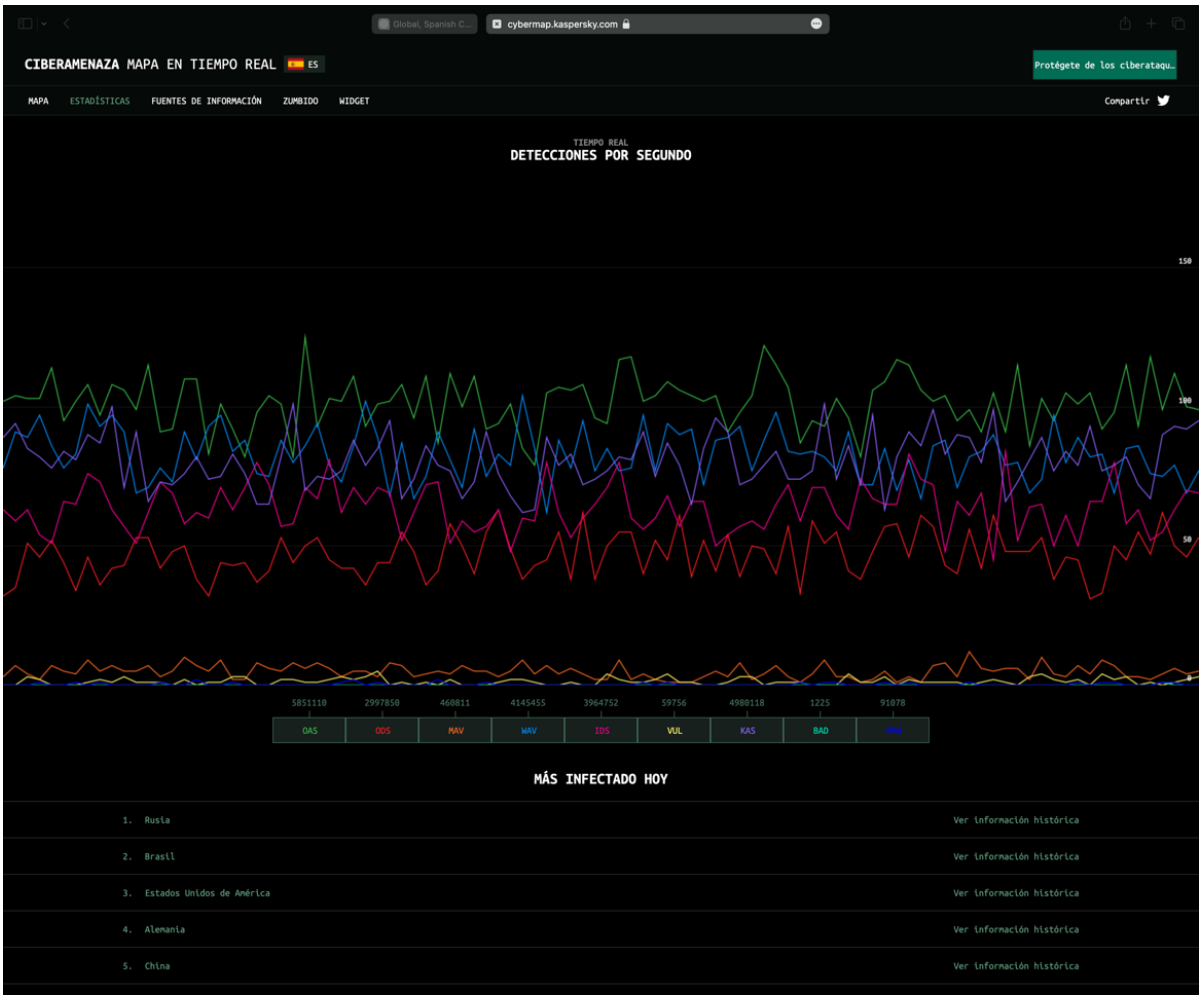
Mapa d'atacs en directe de Kaspersky.

Nota. De Kaspersky, 2023, (https://cybermap.kaspersky.com). Domini públic.

Segons diferents fons d'informació cada dia hi ha milers d'atacs i que aquest nombre augmenta any rere any. Es pot apreciar també en estadístiques d'antivirus, com per exemple, Kaspersky [13], el qual recopila informació sobre les seves deteccions de programari maliciós que fa diàriament i deixa una clara evidencia que les situacions polítiques i de guerra influeixen molt també.

Figura 3

Estadístiques de deteccions per país.



Nota. De Kaspersky, 2023, (https://cybermap.kaspersky.com/stats). Domini públic.

Es pot observar en les estadístiques que la guerra d'Ucraïna està afectant la ciberseguretat a Rússia, amb el qual es pot observar que els grups de hackers aprofiten oportunitats com aquestes per poder efectuar atacs, també es pot apreciar que no només són grups de ciberdelinqüents els que efectuen aquests atacs, perquè es van reportar atacs de Rússia a Ucraïna abans que comencés la guerra, com noves maneres de debilitar un objectiu.[14]

Trobem més exemples d'aquest tipus com podria ser el cas de Stuxnet, el qual és un programari maliciós que es va utilitzar en un atac cibernètic contra l'Iran. Va ser descobert en 2010 i es creu que va ser creat pels governs dels Estats Units i Israel[15]. L'objectiu principal de Stuxnet era danyar els centrifugadors nuclears iranians, que es feien servir pel seu programa nuclear.

El malware es va propagar a través d'una vulnerabilitat en els sistemes informàtics i després es va instal·lar en els sistemes SCADA (Supervisory Control and Data Acquisition) que controlaven els centrifugadors. Una vegada que el malware es trobava en el sistema, va

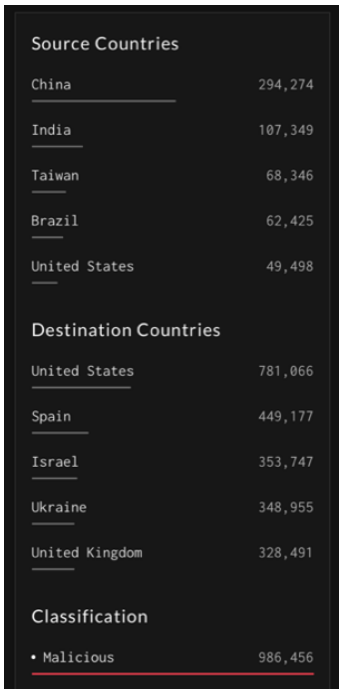
començar a manipular els centrifugadors, accelerant-los i desaccelerant-los de manera repetida, la qual cosa va causar el seu mal irreparable.[15]

Aquest atac és considerat un dels primers i més sofisticats atacs cibernètics en la història i ha estat àmpliament discutit en els mitjans de comunicació i en la comunitat de seguretat cibernètica. És un exemple de com un atac cibernètic pot ser utilitzat per a afeblir un objectiu específic.[15]

També es pot analitzar amb eines gratis que hi ha per internet, com en aquest cas GreyNoise, la qual utilitza honeypots per atraure i detectar amenaces, per després exposar la informació de l'atacant, també recopila informació sobre el seu modus operandi i comportament, per així identificar patrons i tendències en els atacs.[16]

Figura 4

Estadístiques de països que elaboren més atacs.



Nota. De GreyNoise, 2023, (https://viz.greynoise.io/query/?gnql=classification%3Amalicious). Domini públic.

S'observa clarament que ens trobem en una situació de guerra cibernètica i la que més atacs efectua és la Xina.

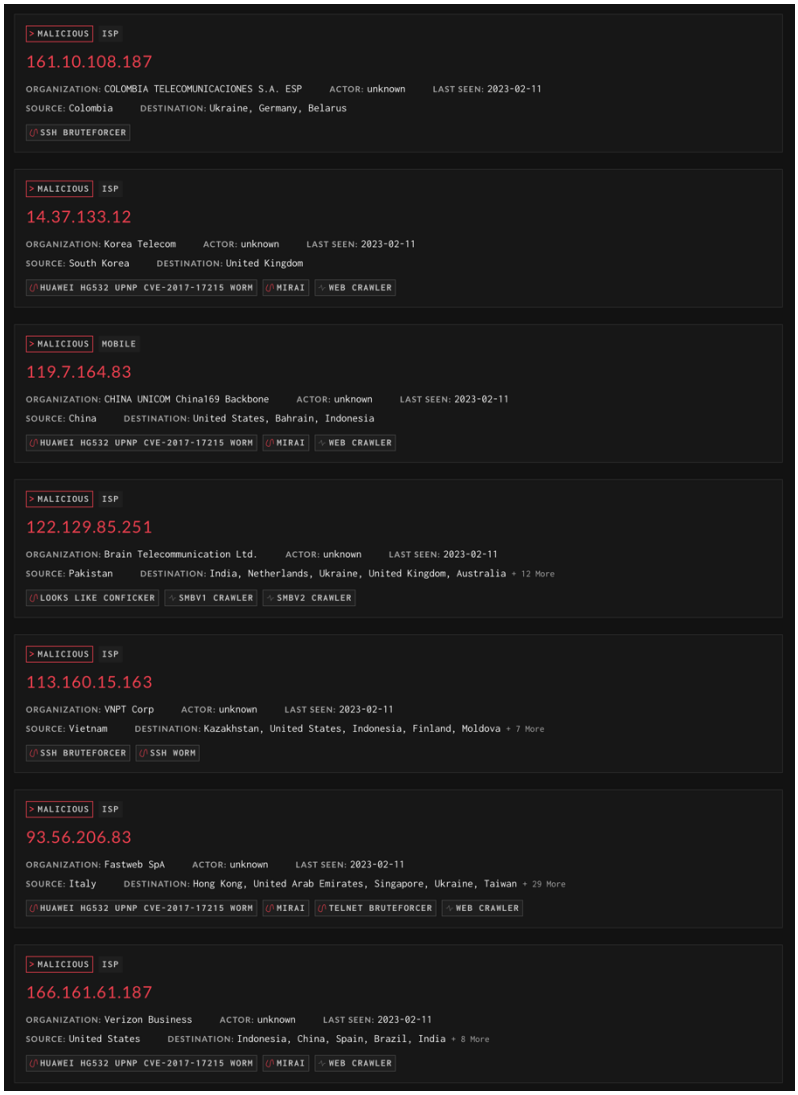
La guerra cibernètica entre la Xina i els EUA és un aspecte important de la relació entre tots dos països. Totes dues nacions han estat involucrades en una intensa disputa cibernètica en els últims anys, amb cadascun acusant l'altre de dur a terme atacs cibernètics amb finalitats polítics i econòmics.[17]

El govern dels EUA ha acusat a la Xina de dur a terme atacs cibernètics en contra d'empreses estatunidenques i de robar secrets comercials i de defensa. El govern xinès, per part seva, ha negat aquestes acusacions i ha acusat els EUA de dur a terme activitats d'espionatge cibernètic.[18][19]

Aquesta guerra cibernètica s'ha intensificat en els últims anys a causa de la importància cada vegada major de la tecnologia i la informació (com s'ha exposat en el punt 1.2) en l'economia global. La disputa cibernètica s'ha convertit en un element clau de la competència geopolítica entre la Xina i els EUA.[20] És important destacar que aquests atacs cibernètics poden tenir greus conseqüències econòmiques i de seguretat per a tots dos països, així com per a altres països i empreses afectats. Per tant, és necessari un enfocament sòlid i col·laboratiu per a abordar aquests desafiaments i protegir els interessos nacionals i globals en l'entorn cibernètic.

Figura 5

Captura de IPs malicioses.



Nota. De GreyNoise, 2023, (https://viz.greynoise.io/query/?gnql=classification%3Amalicious). Domini públic.

Un punt a destacar en aquesta anàlisi és des d'on són produïts aquests atacs cibernètics, ja que la majoria de vegades són elaborats des de les companyies de comunicacions, és a dir, són clients d'aquestes companyies els que elaboren aquests atacs. Amb aquesta anàlisi, sorgeix una pregunta i és: Per què les companyies de comunicacions no bloquegen aquestes IP malicioses? Perquè segurament els clients no saben ni que estan efectuant atacs des dels seus equips, ja que probablement forment part d'una botnet.

Una botnet és una xarxa de dispositius connectats a Internet que han estat infectats i controlats de manera remota sense el coneixement o consentiment dels seus propietaris[21]. Aquests dispositius poden ser computadors, servidors, telèfons mòbils o altres dispositius connectats a Internet. Un atacant pot utilitzar una botnet per a dur a terme una àmplia gamma d'accions malicioses, com a atacs DDoS, spamming, etc[21]. La naturalesa distribuïda d'una botnet significa que els atacs poden ser difícils de detectar i mitigar, i que poden tenir un impacte significatiu en els objectius afectats.

Figura 6

Rànquing d'empreses que elaboren atacs.

Nota. De GreyNoise, 2023, (https://viz.greynoise.io/query/?gnql=classification%3Amalicious). Domini públic.

Podem observar que les empreses amb més atacs efectuats, com hem dit abans són produïts per empreses de telecomunicacions. Podem trobar les empreses "CHINA UNICOM", entre altres empreses xineses, però la més coneguda per a nosaltres és l'empresa de telefònica de brasil, la qual té molt de sentit perquè és el quart país que més atacs efectua al dia d'avui (11/02/2023) i també aquests països al no ser molt desenvolupats tecnològicament, poden tenir més falles de seguretat en els seus equips, sobretot en l'àmbit d'usuari.

Això és un problema, perquè encara que l'atac sigui efectuat des del Brasil, pot ser que el seu origen no sigui aquest país concretament.

2.2. Situació actual a Espanya

Com s'ha esmentat prèviament, la ciberseguretat és un tema de gran preocupació pels països de tot el món. No obstant això, en aquest punt del treball, se centrarà a examinar la situació actual a Espanya. Per a això, ens basarem en l'informe anual sobre criminalitat a Espanya elaborat pel Ministeri de l'Interior del Govern d'Espanya, així com informes elaborats per Deloitte i Google, els quals també aborden la situació de la ciberseguretat al país.

Com podem observar a la Taula 1, es recull el percentatge que representa els cibercrims sobre la criminalitat total, aquests representen una proporció cada cop més gran. Hem de tenir en compte en aquest anàlisi que l'any 2020 va haver-hi un pic més alt que els altres anys, perquè va ser un efecte de la pandèmia de la COVID-19.

Taula 1

Nombre de cibercrims anuals.

2017	5,7%
2018	7,5%
2019	9,9%
2020	16,3%
2021	15,6%

Nota. De Informe sobre la cibercriminalitat a Espanya 2021 (p.23), Javier, L. Francisco, S. David, H. Francisco, M. Marcos, R. Mª Victoria, G. A. Maria, S. M. Ángel, G., 2021, (https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf). Domini públic.

Aquesta taula elaborada pel Sistema Estadístic de Criminalitat (SEC) mostra el comentat anteriorment. S'ha de mencionar que tots aquests càlculs estan fets segons el nombre de cibercrims reportats, és a dir, el nombre d'aquests segurament serà major, perquè com he comentat en el punt 1.2, les empreses no reporten els ciberdelictes o cibercrims patits degut a que aquest acte repercuteixi a la seva reputació.

Observem també en aquest gràfic que els cibercrims van molt en relació amb la utilització de la tecnologia, perquè amb la pandèmia va créixer molt ràpidament la necessitat de digitalitzar-se i les persones van començar a treballar des de casa, el que avui dia es coneix com el teletreball, aquest fet es pot veure reflectit en aquesta taula, perquè l'any 2020 va ser quan es va començar.

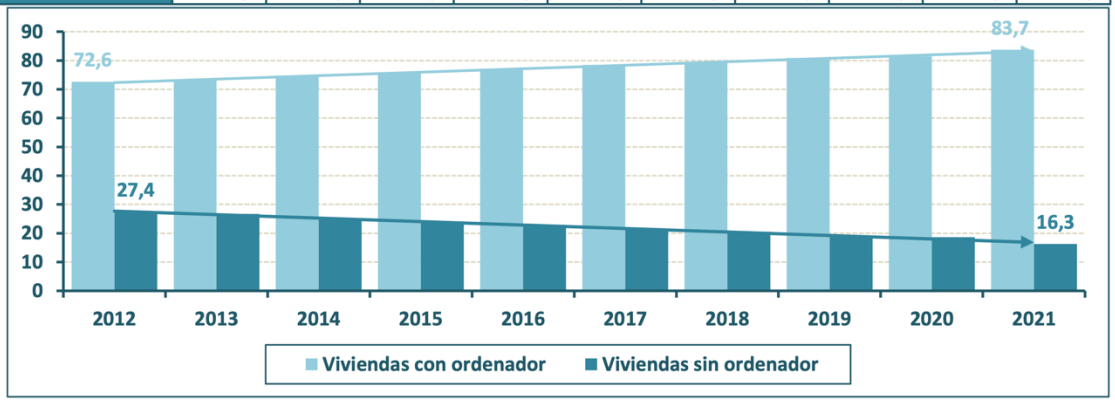
Els cibercrims encara persisteixen, perquè encara es mantenen coses com el teletreball, la digitalització de les empreses, etc. Coses que fan vulnerables a les persones físiques i jurídiques.

En el següent gràfic es pot analitzar el comentat anteriorment, sobre la digitalització i que cada cop les persones tenen més accés a internet i a la tecnologia, fet atractiu pels cibercriminals, perquè hi ha un percentatge cada cop més elevat al qual es pot atacar.

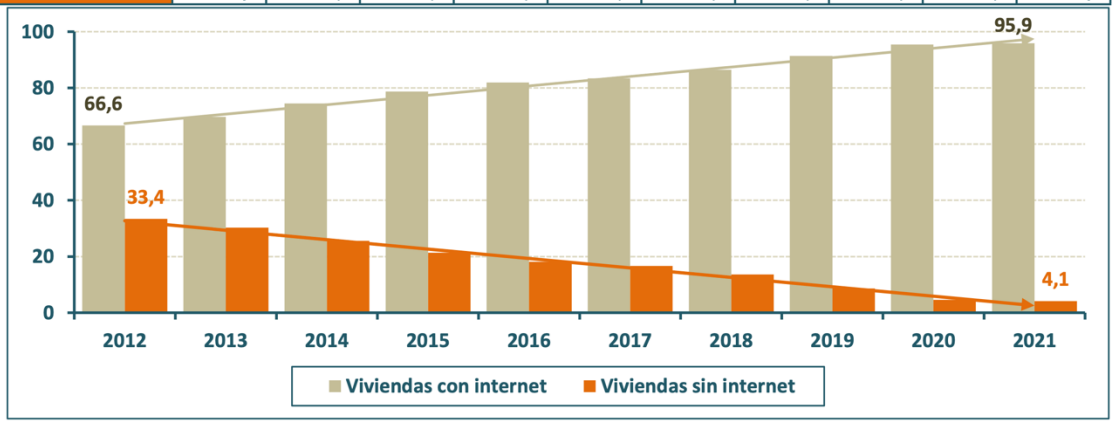
Figura 7 i 8

Gràfiques que mostren l'evolució de la tecnologia a les llars.

PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Viviendas con ordenador	**72,6**	73,3	74,8	75,9	77,1	78,4	79,5	80,9	81,4	**83,7**
Viviendas sin ordenador	**27,4**	26,7	25,2	24,1	22,9	21,6	20,5	19,1	18,6	**16,3**



PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Viviendas con internet	**66,6**	69,7	74,4	78,7	81,9	83,4	86,4	91,4	95,4	**95,9**
Viviendas sin internet	**33,4**	30,3	25,6	21,3	18,1	16,6	13,6	8,6	4,6	**4,1**



Nota. De Informe sobre la cibercriminalitat a Espanya 2021 (p.28), Javier, L. Francisco, S. David, H. Francisco, M. Marcos, R. Mª Victoria, G. A. Maria, S. M. Ángel, G., 2021, (https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf). Domini públic.

Són xifres molt bones de creixement, Espanya és el novè país a la Unió Europea en percentatge de llars amb accés a internet. Efecte de la digitalització, però també implica que s'haurà de saber de protegir-se als nous delictes.

Taula 2

Percentatge de llars amb accés a internet en l'àmbit internacional.

PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
UE (27 países)	75	77	80	81	84	86	88	90	91	92
Bélgica	78	80	83	82	85	86	87	90	91	92
Bulgaria	51	54	57	59	64	67	72	75	79	84
Rep. Checa	73	73	78	79	82	83	86	87	88	89
Dinamarca	92	93	93	92	94	97	93	95	95	96
Alemania	85	88	89	90	92	93	94	95	96	92
Estonia	74	79	83	88	86	88	90	90	90	92
Irlanda	81	82	82	85	87	88	89	91	92	97
Grecia	54	56	66	68	69	71	76	79	80	85
España	67	70	74	79	82	83	86	91	95	96
Francia	80	82	83	83	86	86	89	90		93
Croacia	66	65	68	77	77	76	82	81	85	86
Italia	63	69	73	75	79	81	84	85	88	90
Chipre	62	65	69	71	74	79	82	90	93	93
Letonia	69	72	73	76	77	79	82	85	90	91
Lituania	60	65	66	68	72	75	78	82	82	87
Luxemburgo	93	94	96	97	97	97	93	95	94	99
Hungría	67	70	73	76	79	82	83	86	88	91
Malta	77	78	80	81	81	85	84	86	90	91
Países Bajos	94	95	96	96	97	98	98	98	97	99
Austria	79	81	81	82	85	89	89	90	90	95
Polonia	70	72	75	76	80	82	84	87	90	92
Portugal	61	62	65	70	74	77	79	81	84	87
Rumanía	54	58	61	68	72	76	81	84	86	89
Eslovenia	74	76	77	78	78	82	87	89	90	93
Eslovaquia	75	78	78	79	81	81	81	82	86	90
Finlandia	87	89	90	90	92	94	94	94	96	97
Suecia	92	93	90	91	94	95	92	96	94	93
Reino Unido (*)	87	88	90	91	93	94	95	96	97	97

Nota. De Informe sobre la cibercriminalitat a Espanya 2021 (p.33), Javier, L. Francisco, S. David, H. Francisco, M. Marcos, R. Mª Victoria, G. A. Maria, S. M. Ángel, G., 2021, (https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf). Domini públic.

A Espanya hi ha diversos òrgans que es dediquen a evitar i resoldre problemes de ciberseguretat, els quals són:[22]

- **Oficina de Coordinació de Ciberseguretat (OCC):** És l'òrgan tècnic de coordinació del Ministeri de l'Interior en matèria de ciberseguretat, exerceix com a canal específic de comunicació entre els Centres de Resposta a Incidents de Seguretat Informàtiques nacionals de referència i la Secretaria d'Estat de Seguretat, exercint la coordinació tècnica en matèria de ciberseguretat entre aquesta Secretaria d'Estat i els seus organismes dependents.

- **INCIBE-CERT:** És un dels equips de resposta de referència davant incidents que es coordina amb la resta dels equips nacionals i internacionals per a millorar l'eficàcia en

la lluita contra els delictes que involucren a les xarxes i sistemes d'informació, reduint els seus efectes en la seguretat pública.

- **CCN-CERT:** Organisme responsable de coordinar l'acció dels diferents organismes de l'Administració que utilitzin mitjans o procediments de xifra i garantir la seguretat de les Tecnologies de la Informació en aquest àmbit.

Tots tres òrgans són els responsables de gestionar incidents en l'àmbit nacional, per així poder reduir l'abast dels atacs a les víctimes. També en haver-hi dits òrgans es pot reduir l'interès dels cibercriminals, ja que són mesures de mitigació.

A la Taula 3 podem observar la tipologia dels incidents ocasionats i els quals van ser gestionats per l'òrgan INCIBE-CERT:

Taula 3

Incidents gestionats pel INCIBE-CERT.

Tipo de incidente	INCIDENTES GESTIONADOS					
	2016	2017	2018	2019	2020	2021
Intrusión	14.373	19.275	8.541	6.479	9.557	7.039
Fraude	11.843	11.959	55.932	31.938	42.641	31.213
Malware	76.811	81.090	27.016	27.358	46.893	32.605
SPAM	10.279	7.957	0	0	0	0
Disponibilidad	495	514	100	58	1.971	7.177
Intento de intrusión	381	1.435	396	1.518	1.289	1.753
Robos de información	37	47	63	77	161	920
Contenido Abusivo			9.353	4.064	2.986	5.253
Recolección de información			5.605	84	87	106
Sistema Vulnerable			3.731	31.414	23.161	20.609
Otros	1.038	787	782	4.407	4.409	2.451

Nota. De Informe sobre la cibercriminalitat a Espanya 2021 (p.40), Javier, L. Francisco, S. David, H. Francisco, M. Marcos, R. Mª Victoria, G. A. Maria, S. M. Ángel, G., 2021, (https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf). Domini públic.

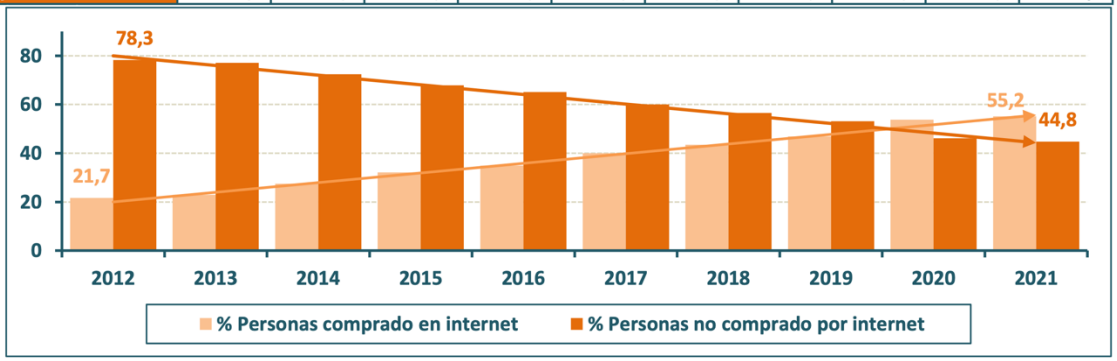
Els que tenen més freqüència són els de frau i malware, ja que com he comentat anteriorment hi ha cada cop més ordinadors i gent amb accés a internet, el qual fa que ocorrin més aquesta classe d'esdeveniments. El frau es pot explicar per què en haver-hi més gent que utilitza tecnologia al seu dia a dia, pot fer coses convencionals com comprar per internet, però no sempre totes les fonts són de fiar.

Podem veure en el següent gràfic l'augment de les persones que han fet alguna compra a internet:

Figura 9

Percentatge de persones que han comprat per internet algun cop.

	% PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Comprado en internet	**21,7**	22,9	27,5	32,1	34,9	40,0	43,5	46,9	53,8	**55,2**
No comprado en internet	**78,3**	77,1	72,5	67,9	65,1	60,0	56,5	53,1	46,2	**44,8**



Nota. De Informe sobre la cibercriminalitat a Espanya 2021 (p.32), Javier, L. Francisco, S. David, H. Francisco, M. Marcos, R. Mª Victoria, G. A. Maria, S. M. Ángel, G., 2021, (https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf). Domini públic.

Hi ha cada cop més gent que compra a internet i no tothom té uns coneixements mínims d'informàtica, com per poder identificar si un lloc pot ser menys fiable o més. Els ciberdelinqüents aprofiten aquest fet per poder lucrar-se d'aquesta gent. Recordem que aquesta gent és la mateixa que treballa a les empreses.

Segons un report fet per Google i The Cocktail Analysis pel 75%[23] dels usuaris a Espanya considera que la ciberseguretat és molt important, però 4 de cada 10 usuaris[23] considera que té un nivell baix de protecció, és a dir, el 40%[23] considera que els seus dispositius no estan prou protegits. També un 60%[23] de les persones entrevistades han patit una incidència relacionada amb la seguretat.

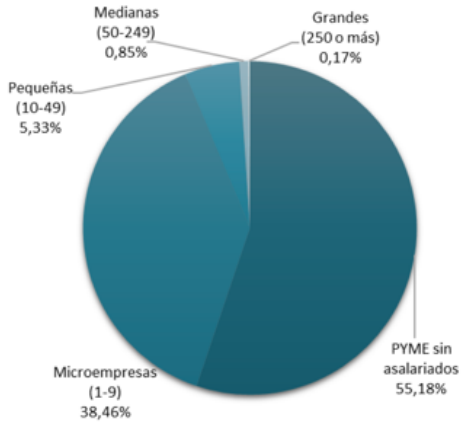
En aquest report observem que la població té un mínim de coneixement sobre la ciberseguretat, però no és suficient.

- Només un 26%[23] utilitza contrasenyes diferents en cada lloc web.
- Un 21%[23] de les persones tenen una còpia de seguretat dels seus arxius.
- Ens trobem que el 14%[23] de les persones actualitza les seves contrasenyes amb regularitat.
- Són vagament coneixedors sobre protocols de seguretat, però quan si els ha explicat sobre ells, un gran percentatge afirma saber del que es tracta[23].

En conclusió, un dels reptes del país és la conscienciació sobre la ciberseguretat i el que són unes bones pràctiques, per així poder millorar la seguretat dels usuaris.

Figura 10

Distribució d'empreses per mida.



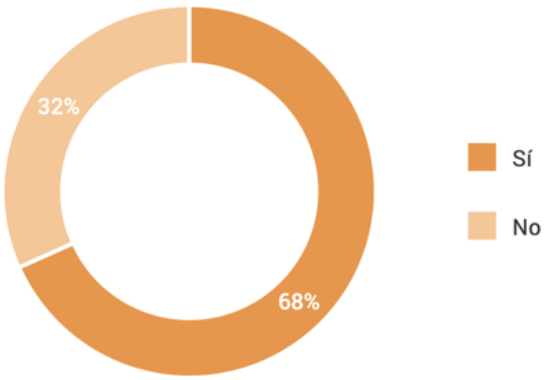
Nota. De Cifras PYME Datos enero 2022 (p.1), Govern d'Espanya, 2022, (http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-enero2022.pdf). Domini públic.

Pel que fa a les empreses a Espanya analitzarem les PIMES, ja que és el tipus d'empresa més freqüent a aquest país, com podem observar en la Figura 10.

És molt destacable l'escàs nivell de seguretat que tenen les empreses, ja que els responsables de seguretat de les PIMES entrevistades, només el 12%[23] assegura que la seva seguretat és molt alta.

Figura 11

Percentatge de PIMES que saben que es la ciberseguretat.



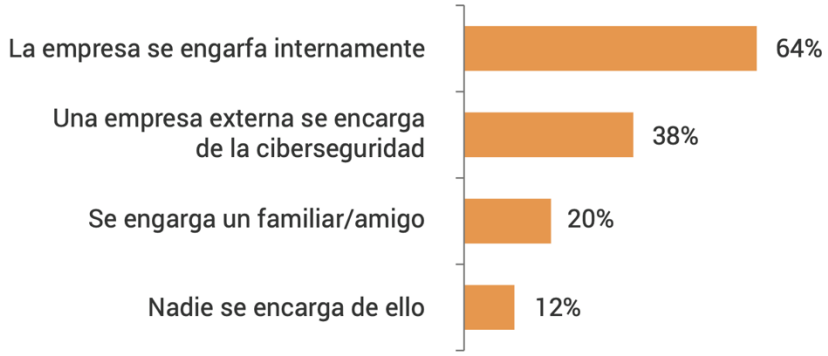
Nota. De Panorama actual de la Ciberseguridad en España (p.55), The Cocktail Analysis, 2022, (https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf). Domini públic.

Un 51%[23] de les empreses atribueix el concepte de la ciberseguretat només com a actuacions a la xarxa enfront de tercers, és a dir, virus informàtics i només el 21%[23] ho atribueix com a seguretat informàtica i una manera de protegir les seves dades.

També un altre punt a tractar és que les PIMES no externalitzen el seu acompliment en ciberseguretat, el 64%[23] de les empreses analitzades al report de Google porten la ciberseguretat internament a l'empresa, el 20%[23] s'encarrega un familiar o amic i un 12%[23] no es preocupa per a la seva ciberseguretat a l'empresa. Només el 38%[23] de les empreses analitzades externalitzen el seu acompliment en ciberseguretat.

Figura 12

Percentatge de com es gestiona la ciberseguretat a les PIMES.



Nota. De Panorama actual de la Ciberseguridad en España (p.56), The Cocktail Analysis, 2022, (https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf). Domini públic.

Les mesures de seguretat també tenen les seves carències, ja que només el 44%[23] de les empreses actualitzen els ordinadors i mòbils, uns altres només un dels dos i la resta cap. També hi ha problemes amb el sistema de verificació de doble factor, pel fet que un 31%[23] de les empreses no l'acaben d'implementar. Però la més preocupant és sobre la desconfiança en els serveis al núvol, perquè un 51%[23] no es fia en absolut o té poca confiança, factor important perquè les organitzacions que es dediquen al sector tenen equips especialitzats que es dediquen a la seguretat dels seus servidors i infraestructures, que una PIME no pot fer.

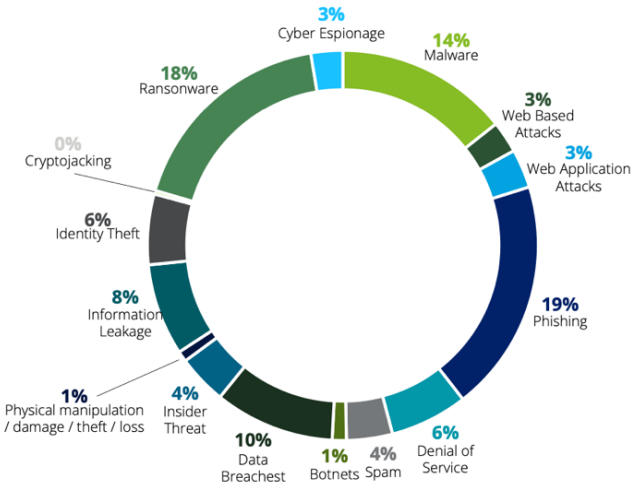
Un altre punt molt important, el qual si es millora es podria millorar amb escreix la situació, és la conscienciació sobre la ciberseguretat, ja que només un 30%[23] dels responsables d'informàtica consideren que els seus empleats estan conscienciats sobre la importància de la ciberseguretat.

La ciberseguretat ha de ser un punt fort a les empreses, ja que és un fet real que la teva empresa pot patir un àtac, amb la mateixa facilitat que s'atraca una botiga al carrer, però personalment crec que té més repercussió. L'informe elaborat per Deloitte exposa que l'any 2022 s'han detectat un 26%[25] més ciberincidents que a l'any anterior i hi ha empreses que han patit més d'un incident crític de ciberseguretat.

En el mateix informe s'exposen les amenaces més habituals a les empreses a Espanya, en les quals podem veure molt destacades dues d'elles, el phishing (mètode d'enginyeria social per poder accedir a l'empresa) i el ransomware (malware).

Figura 13

Percentatge d'amenaces més habitual.



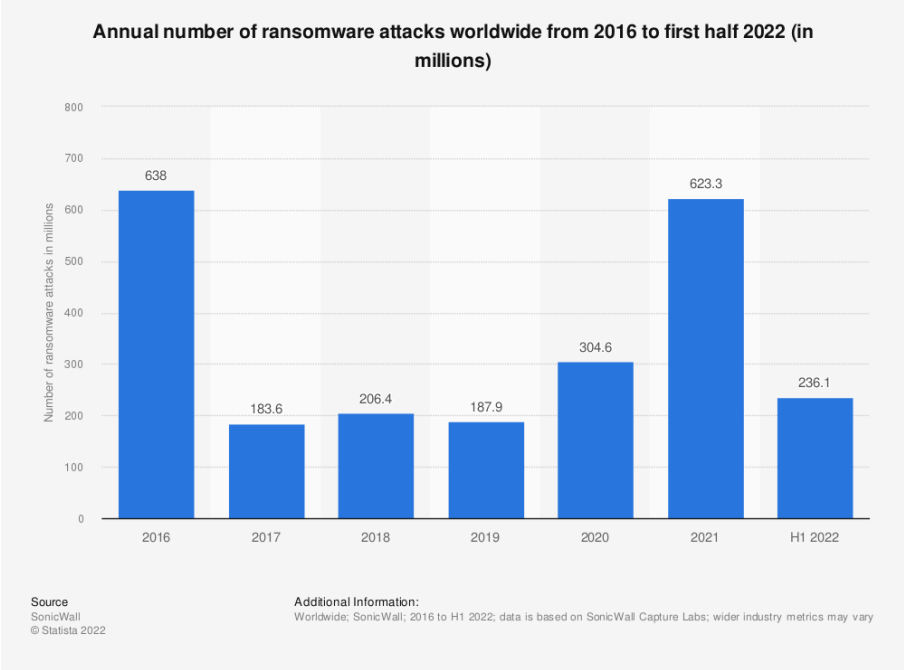
Nota. De Informe Cibercriminalidad 2021 (p.42), Carmen, S. César, M. Gianluca, D. Miguel, O. Alejandro, V., 2021, (https://www2.deloitte.com/content/dam/Deloitte/es/Documents/riesgos/deloitte-es-risk-advisory-estado-de-la-ciberseguridad-en-espana-2022.pdf). Domini públic.

Els ransomware són cada cop més utilitzats per atacar a les empreses. Un ransomware és un tipus de programari maliciós que es fa servir per a bloquejar l'accés a les dades d'un sistema informàtic o dispositiu, i després exigir un rescat per a restaurar l'accés.

Podem veure la seva evolució amb els anys en la Figura 14, hem de tenir en compte que l'any 2022 encara no estan tots els atacs registrats.

Figura 14

Nombre anual de atacs Ransomware (2016-2022)



Nota. De Statista, SonicWall, 2021, (https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/), Domini públic.

Les empreses es dedicaven a pagar el rescat de les seves dades, perquè no volia perdre reputació en el mercat i conseqüentment perdre clients, ja que com he comentat en un punt anterior la llei a Espanya de no notificar aquest delicte té una multa que encara funciona amb pessetes, un motiu més per no notificar-lo. Podem veure a la pàgina RANSOMWHARE la quantitat de diners que s'ha recopilat gràcies a aquests tipus d'atacs, al dia d'avui (19/02/2023) hi ha recaptats 197,536,611.98$[27], un xifra molt elevada. Afortunadament segons la font "Business Insider" estima que més d'un 40%[28] de les empreses ja no paga els rescats.

Com a breu conclusió, es podria arribar que gràcies a les notícies dels àtacs produïts hi ha una conscienciació cada cop més gran sobre la ciberseguretat, per aquest motiu les empreses comencen a invertir més a protegir els seus actius intangibles (dades) i no acabar pagant el rescat, ja que amb aquest acte s'està finançant a aquestes bandes criminals.

2.3. Necessitat de trobar talent a les empreses

La ciberseguretat és una disciplina crítica per a la protecció d'informació, sistemes i xarxes informàtiques. A mesura que la tecnologia avança i els ciberatacs es tornen cada vegada més sofisticats, s'ha tornat més important que mai comptar amb professionals capacitats en ciberseguretat. No obstant això, hi ha una escassetat significativa de talent en el camp a causa d'una sèrie de factors.

Un dels principals factors que contribueixen a la falta de talent en ciberseguretat és la demanda creixent d'aquests professionals a tot el món. A mesura que les empreses i organitzacions de totes les grandàries busquen protegir els seus actius digitals i dades confidencials, la necessitat de professionals de ciberseguretat s'ha disparat en els últims anys. Com a resultat, molts ocupadors estan lluitant per trobar candidats qualificats per a cobrir els seus llocs de treball en ciberseguretat.

A més, el camp de la ciberseguretat és molt tècnic i requereix habilitats específiques i coneixements especialitzats en àrees com a criptografia, anàlisi de vulnerabilitats, gestió de riscos i resposta a incidents, entre altres. No hi ha suficients programes educatius o de capacitació en ciberseguretat per a satisfer la creixent demanda de professionals altament capacitats.

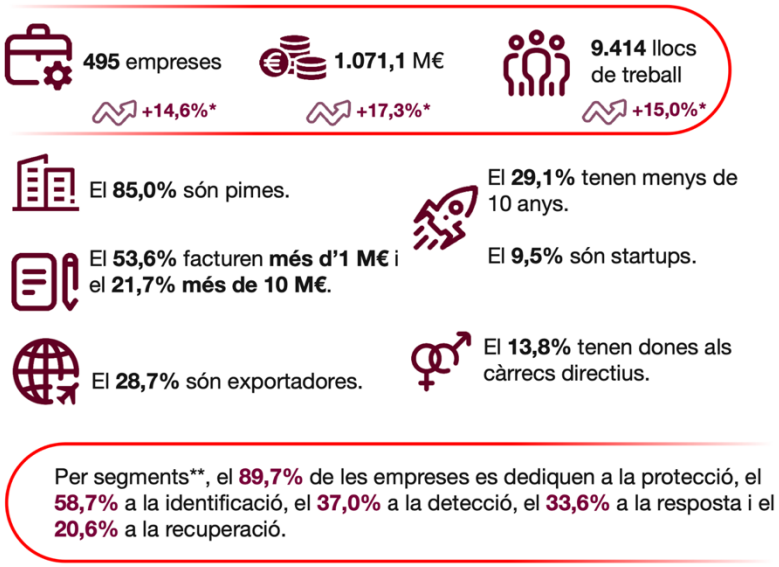
També existeix un problema de retenció de talent en el camp de la ciberseguretat. Els professionals altament capacitats en ciberseguretat sovint són atrets per salaris i beneficis més atractius en altres indústries com la tecnologia i el comerç. Això significa que fins i tot si es troben talents capacitats per a treballar en ciberseguretat, pot ser difícil per a les empreses i organitzacions retenir-los a llarg termini.

Per aquest punt tractarem la falta de talent que hi ha a reu del món en l'àrea de la ciberseguretat. Segons l'informe de Deloitte citat en el punt anterior, el 81%[25] dels CISO i els responsables de ciberseguretat de les empreses considera que no disposa de suficient personal, això és perquè les necessitats de les empreses en aquest àmbit creixen cada any i genera una demanda superior a l'oferta, concretament hi ha una bretxa de professionals d'un 26%[25].

Es pot veure reflectida aquesta falta de talent per l'increment de màsters, postgraus i formacions professionals, ja que s'ha de complir aquesta demanda tan forta de talent. S'ha de mencionar que a Catalunya la bretxa és molt major, un 57%[29] perquè s'han creat 495[29] empreses que es dediquen a la ciberseguretat.

Figura 15

Resum sobre les empreses de seguretat a Catalunya.



Nota. De Ciberseguretat a Catalunya 2023 (p.33), Generalitat de Catalunya, 2023, (https://www.accio.gencat.cat/web/.content/bancconeixement/documents/pindoles/ACCIO-ciberseguretat-a-catalunya-pindola-tecnologica-ca.pdf). Domini públic.

3. Com es pot transformar una persona en un ciberdelinqüent?

Amb l'augment dels ciberdelictes i l'evolució de la tecnologia s'ha pogut observar que els grups criminals utilitzen noves tecnologies per elaborar atacs, però a part també tenen noves oportunitats de negoci, els quals ja no només són del que guanyen amb les víctimes, sinó que també guanyen diners amb el lloguer de les seves pròpies eines d'atac (productes as a Service).

Un dels serveis més notoris que ofereixen les organitzacions criminals és el Ransomware as a Service (RaaS). Aquest model de negoci permet als ciberdelinqüents que no tenen els coneixements tècnics i recursos per a desenvolupar el seu propi programari de ransomware, puguin accedir a eines i serveis especialitzats que els permeten llançar atacs de ransomware amb facilitat.

Les organitzacions criminals ofereixen aquests serveis de RaaS a altres delinqüents, els qui paguen una tarifa per utilitzar el programari i els serveis associats per fer els seus propis atacs. A canvi, els proveïdors de RaaS s'emporten una part dels ingressos assolits pels atacants. Aquest model de negoci ha demostrat ser molt efectiu per als delinqüents, ja que els permet escalar ràpidament les seves operacions i arribar a un públic més ampli, sense haver d'invertir temps i esforç en la creació d'eines i serveis de ransomware.

L'augment del RaaS és només una mostra de la creixent sofisticació de les organitzacions criminals en el món digital. A mesura que la tecnologia continua avançant i els delinqüents troben noves maneres d'explotar-la, és important que les empreses i els individus prenguin mesures per a protegir-se d'aquestes amenaces.

3.1. Requisits mínims per poder operar amb els programes maliciosos

Durant aquest punt, observarem els requisits mínims que hi ha per poder operar amb programes maliciosos, transformant-te així en un cibercriminal o ciberdelinqüent depenen del que arribis a fer amb dites eines.

3.1.1. Requisits obligatoris

1. **Coneixement d'informàtica:** Definitivament has de tenir uns coneixements d'informàtica per poder utilitzar segons quines eines, però només han de ser coneixements d'usuari bàsic i saber com buscar per internet, perquè hi ha molta informació la qual et pot facilitar instruccions.

2. **Disposar d'un ordinador:** Aquest ordinador no ha de ser realment potent, però es recomana que aquest tingui unes especificacions elevades, sobretot per a la comoditat del usuari. Les especificacions de l'ordinador poden ser:

    a. Bàsiques: Processador Intel i5 o equivalències com el Ryzen 5 (a ser possible de generacions actuals), memòria RAM de 16 GB i amb la GPU integrada del processador.

b. Avançades: Processador Intel i9 o equivalències com el Ryzen 9, memòria RAM de 32 GB i amb la GPU integrada del processador.

Aquestes especificacions són merament personals, ja que amb aquestes es pot treballar còmodament, és a dir, es pot utilitzar encara un ordinador amb especificacions més ajustades, com podria ser un processador Intel i3 amb 4 GB de RAM, però es faria més tediós treballar amb un equip d'aquestes característiques.

3. **Connexió a la xarxa:** Evidentment s'ha de disposar d'una connexió a la xarxa per poder operar. Qualsevol operador local es bo per poder gaudir d'una connexió (no necessàriament ha de ser teva).

4. **Tor (*The Onion Encaminador*):** És una xarxa de comunicacions anònima i descentralitzada que permet als usuaris navegar per Internet de manera segura i privada[30]. Les seves funcions principals són:

   - Ocultar l'adreça IP de l'usuari i la seva ubicació geogràfica.
   - Encriptar el trànsit d'Internet de l'usuari per a protegir la seva privacitat.
   - Redirigir el trànsit a través d'una xarxa de nodes distribuïts a tot el món per a dificultar el rastreig i la identificació dels usuaris.

   Dita xarxa de comunicació anònima no és l'única, ja que hi ha varies més com podrien ser Freenet, ZeroNet o I2P.

5. **Programari de virtualització:** És un programa que permet crear una o més màquines virtuals (VM) en una computadora física. Una màquina virtual és una simulació d'una computadora completa, que inclou un sistema operatiu, programes i recursos de maquinari virtual, com a memòria, processador, emmagatzematge i dispositius d'entrada/sortida.

   El programari de virtualització funciona per crear una capa d'abstracció entre el maquinari físic de la computadora i el sistema operatiu i aplicacions que s'executen en la VM. Això permet que diverses VMs puguin executar-se en una mateixa computadora física, cadascuna amb el seu propi sistema operatiu i aplicacions, com si estiguessin executant-se en la seva pròpia computadora[34].

   Exemples: VirtualBox, Citrix XenServer, Sandboxie, VMware Workstation Pro, Cameyo, Parallels, etc.

3.1.2. Requisits opcionals (recomanables)

1. **VPN:** Una VPN (*Virtual Private Network*) és un tipus de connexió de xarxa, la qual permet als usuaris connectar-se a Internet de manera segura i privada[31].

La VPN xifra la connexió entre el dispositiu de l'usuari i la xarxa a la qual es connecta, cosa que significa que la informació que s'envia a través de la VPN està protegida i no pot ser vista per tercers[31].

Exemples: ExpressVPN, NordVPN, CyberGhost VPN, Surfshark, Private Internet Access (PIA), Hotspot Shield, ProtonVPN, Windscribe, VyprVPN, TunnelBear, IPVanish, etc.

2. **SO Tails:** És un sistema operatiu basat en Linux que està dissenyat per a protegir la privacitat i l'anonimat en línia. Tails és un acrònim de "*The Amnesic Incognito Live System*" i és conegut per la seva capacitat d'executar-se des d'un USB o DVD, cosa que significa que no necessita instal·lar-se en un ordinador per a ser utilitzat.

   Tails inclou diverses eines de privacitat i seguretat, com Tor, que permet navegar per la web de manera anònima, i una suite de xifratge que permet xifrar i desxifrar arxius i correus electrònics. Tails també s'esborra automàticament de la memòria després que l'usuari tanca la sessió, la qual cosa el fa especialment útil per a activitats en línia que requereixen un alt nivell de privacitat, com accedir a la *Dark web*[32][33].

3.2. Com entrar a la coneguda "*Dark Web*"?

En aquest punt del treball es farà una demostració pràctica de com poder accedir-hi a la *Dark Web* o més coneguda com la *Deep Web*, error comú, ja que no tenen el mateix significat.

La *Deep Web* es refereix a qualsevol part d'internet que no està indexada pels motors de cerca convencionals. Això pot incloure contingut protegit per contrasenya, pàgines d'inici de sessió, bases de dades privades i contingut dinàmic generat per usuari.

La *Dark Web*, d'altra banda, són totes aquelles pàgines que directament estan ocultes, s'accedeix a elles des de xarxes privades i encriptades com Tor. La *Dark Web* és coneguda per ser un lloc on es poden fer activitats il·legals, com la venda de drogues, armes, informació robada, etc. també és un refugi per a l'activitat criminal organitzada.

3.2.1. Eines utilitzades per a la prova pràctica

Hardware: Per fer aquesta prova s'ha utilitzat un ordinador amb un processador Intel i5 de quarta generació, 8 GB de RAM, la ROM integrada del mateix processador i una memòria extraïble de 16 GB.

Software: Durant aquesta prova s'han utilitzat només dues eines de les esmentades anteriorment, per fer que la pràctica sigui més senzilla. Les eines que s'utilitzaran seran les següents: Tor i SO Tails.

3.2.2. Accés a la "*Dark web*"

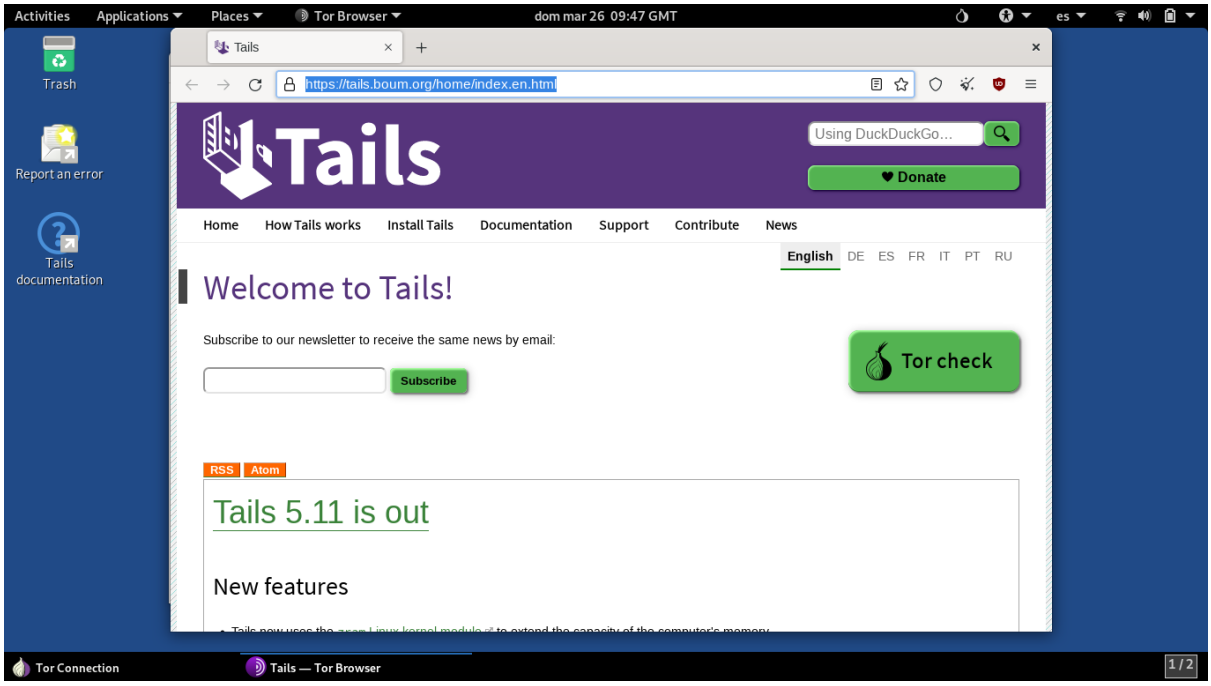
L'accés a aquesta internet oculta no és tant difícil com ho pot semblar. En el meu cas particular, com he nombrat anteriorment, he utilitzat el sistema operatiu "Tails" el qual també té el navegador "Tor" preinstal·lat.

Aquest sistema operatiu s'instal·la de la següent manera (en cas de ser una màquina amb el sistema operatiu Windows)[35]:

En mode d'instruccions, per si algú ho vol fer:

1. **Descarregar l'arxiu ISO de Tails:** El primer que cal fer és descarregar l'arxiu ISO de Tails des del lloc web oficial. S'ha de seleccionar l'opció d'instal·lació per a Windows i donar a descarregar, un cop feta la descàrrega pots verificar dins de la mateixa web si l'arxiu s'ha descarregat sense problemes.
2. **Descarregar i instal·lar el programari d'enregistrament d'imatge:** Aquest pas es pot fer paral·lelament amb l'anterior. A la mateixa web li dones a descarregar al programa balenaEtcher i un cop finalitzada la descàrrega l'instal·les.
3. **Inserir la unitat USB:** Connecta la unitat USB a l'ordinador on desitges instal·lar Tails. Assegura't que la unitat USB tingui almenys 8 GB d'espai disponible i que estigui formatat en el format "*FAT32*".
4. **Executar el programa balenaEtcher:** Un cop fet els passos anteriors s'ha d'executar el programa balenaEtcher, donant doble clic a l'executable.
5. **Seleccionar la imatge ISO de Tails:** Un cop executat el programa, selecciones la imatge ISO on la tinguis guardada.
6. **Instal·lar el SO a la memòria USB:** Un cop seleccionat el sistema operatiu, passes a seleccionar la unitat USB que tens a l'equip.
7. **Crear la unitat USB Tails:** Un cop seleccionats l'arxiu del SO i la unitat on ho vols instal·lar, prems el botó de "*Flash!*".
8. **Reiniciar la computadora:** Ara ja que està instal·lat el SO a la unitat USB, passa a reiniciar l'ordinador.
9. **Configurar l'arrencada de la computadora:** Mentre s'està reiniciant has d'accedir a la BIOS de l'ordinador, en el meu cas amb el botó F2 (has de buscar com s'ha d'accedir-hi al teu). Un cop dins de la BIOS, s'ha d'anar a les opcions d'arrancada i canviar l'ordre de les unitats, és a dir, posar la unitat flash com a primera opció.
10. **Arrencar des de la unitat USB:** Un cop canviat l'ordre d'arrancada, has d'anar l'últim apartat de tots del menú i donar-li a l'opció de guardar canvis i reiniciar.

Un cop fets aquests passos i s'entra a Tails (fas els passos previs per utilitzar el sistema operatiu) et quedes en el punt de la imatge següent:



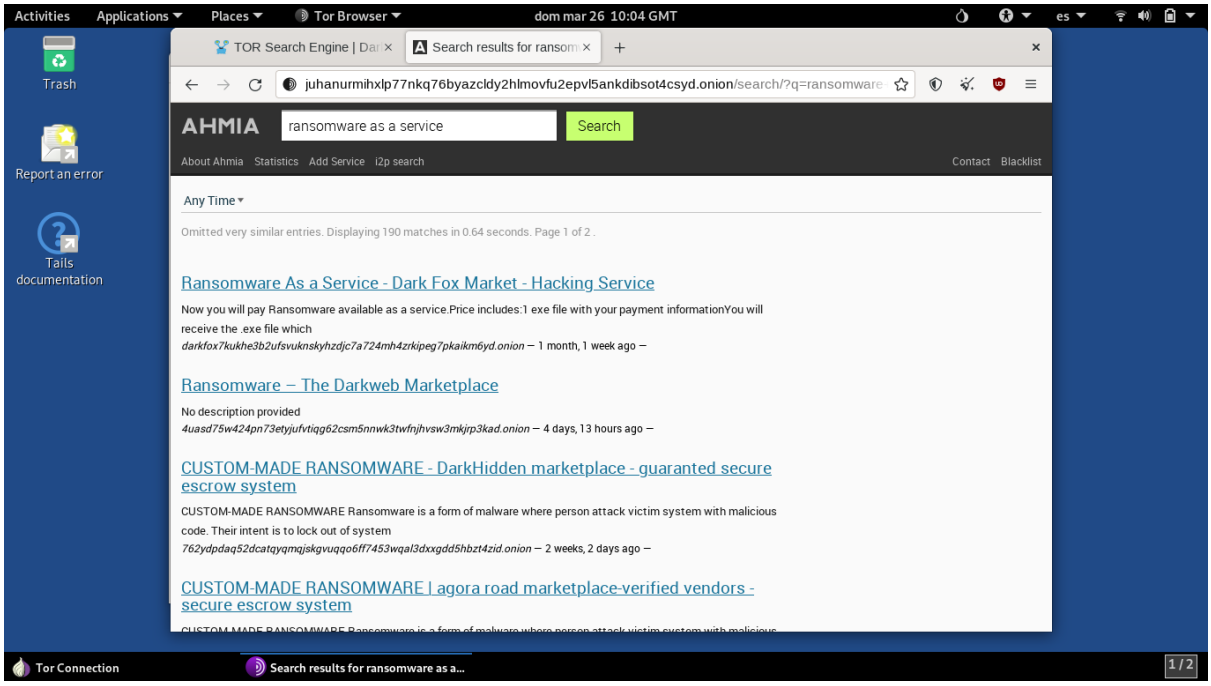
3.3. Com formar part d'una organització de ciberdelinqüents?

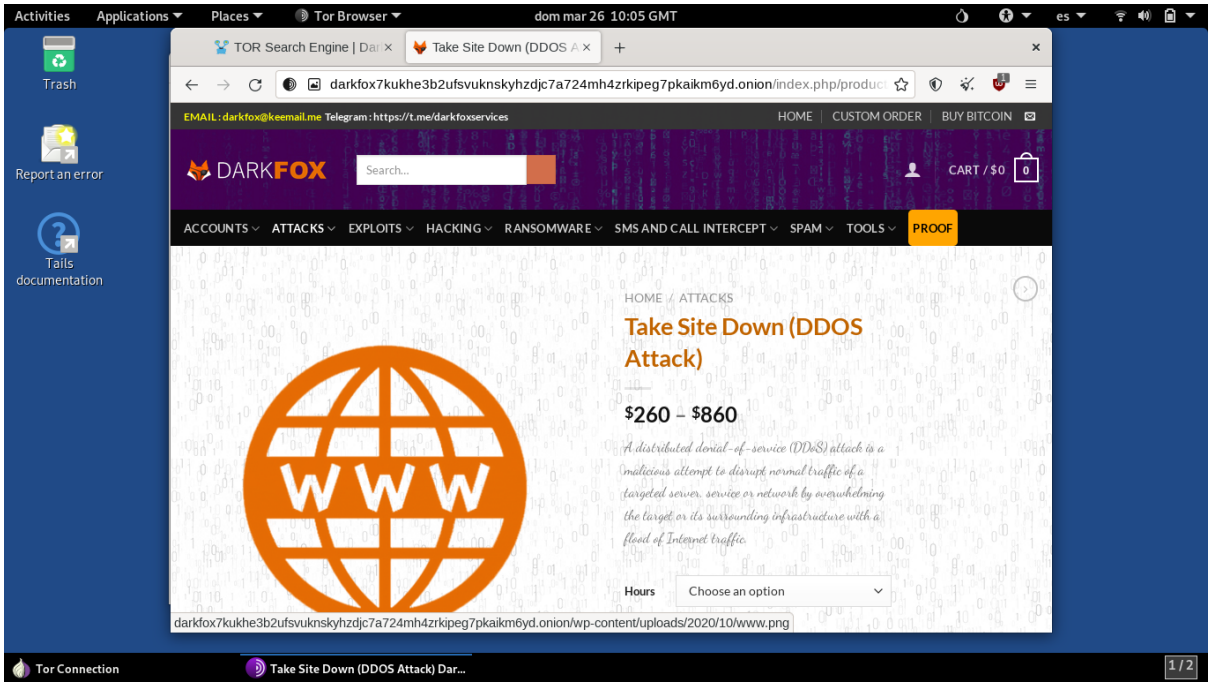
En aquest punt del treball s'ha explorat la *Dark Web* per a comprendre millor com operen els ciberdelinqüents en entorns ocults i anònims. És important destacar que la *Dark Web* no és accessible des de navegadors convencionals i requereix eines i tecnologies específiques per a accedir a ella. Per aquesta raó, no es pot fer referència directa a la informació obtinguda en aquesta secció del treball.

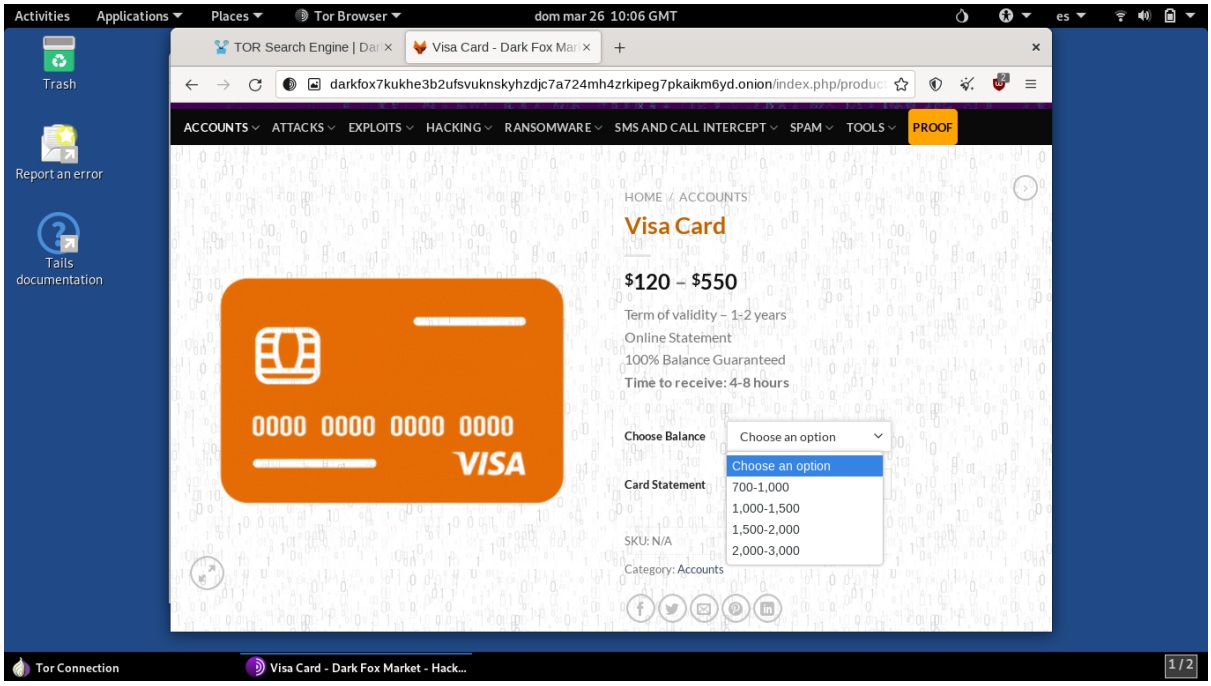
Navegar per la *Dark Web* no és tan senzill com en les pàgines web convencionals. Es requereixen eines i tecnologies específiques, així com enllaços directes als llocs web ocults i anònims. Per a facilitar la meva exploració, vaig utilitzar un cercador anomenat "AHMIA". Encara que pot ser desafiador, els coneixements adquirits en aquesta exploració són essencials per a comprendre la naturalesa de la ciberdelinqüència i les amenaces que representa per a la seguretat en línia.

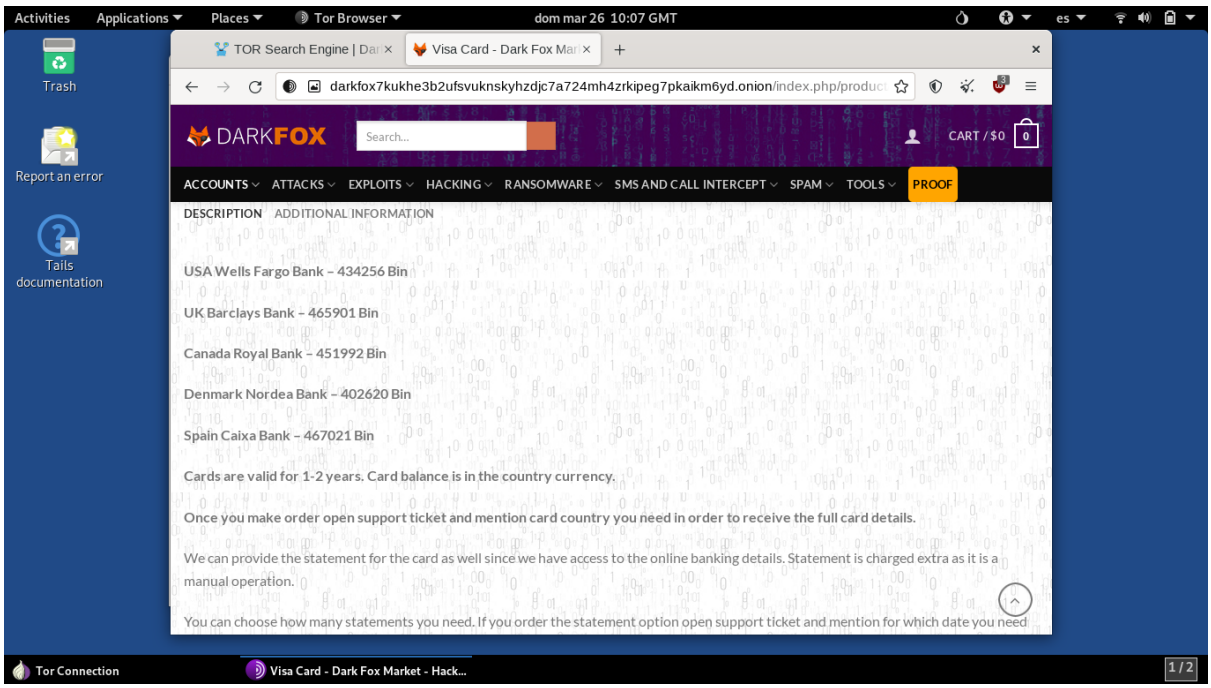
En la *Dark Web* he descobert múltiples llocs web dedicats a activitats il·legals. Entre ells, *Marketplaces* que venen targetes VISA, armes, virus i comptes de desenvolupadors per a l'Apple Store, que podrien ser utilitzades per a crear aplicacions malicioses de manera discreta. També he trobat la pàgina web d'un hacker, el qual ofereix els seus serveis de manera clandestina per un preu accessible i pàgines web que exposen informació de les empreses que no van pagar el rescat del Ransomware. Aquestes troballes destaquen la facilitat amb la qual els ciberdelinqüents poden accedir a recursos per a dur a terme activitats il·legals i la importància d'implementar mesures de seguretat efectives per a protegir-se contra elles.

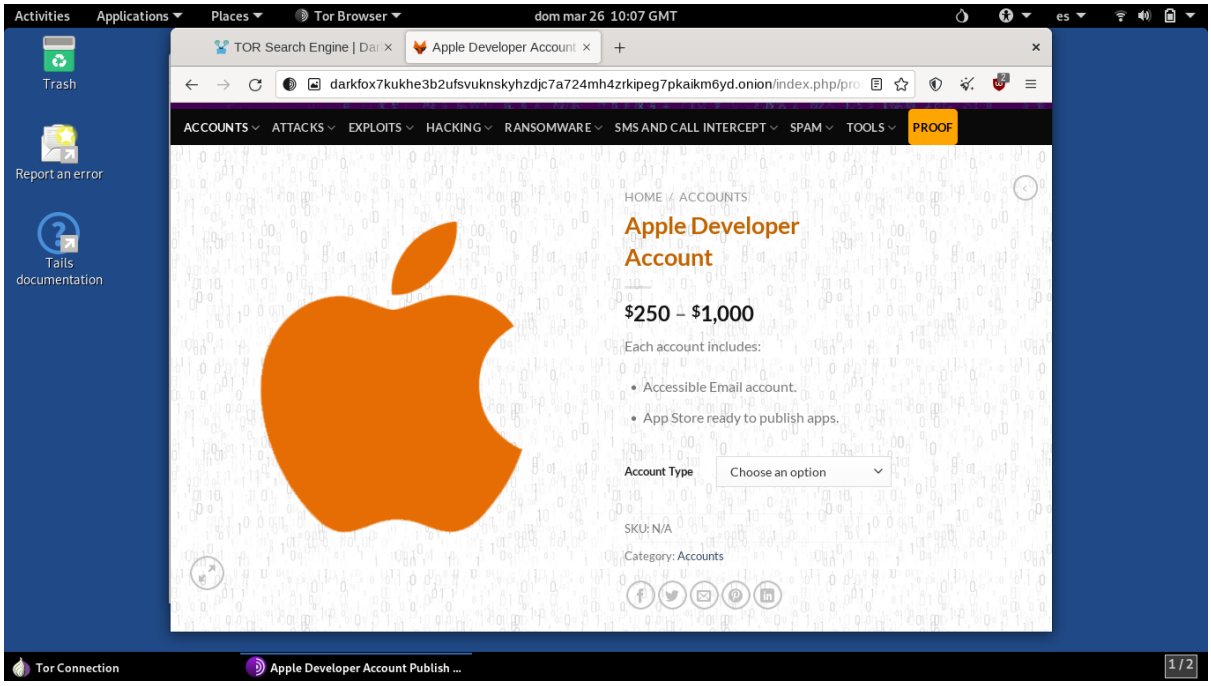
A continuació, aquestes imatges mostren les pàgines citades:

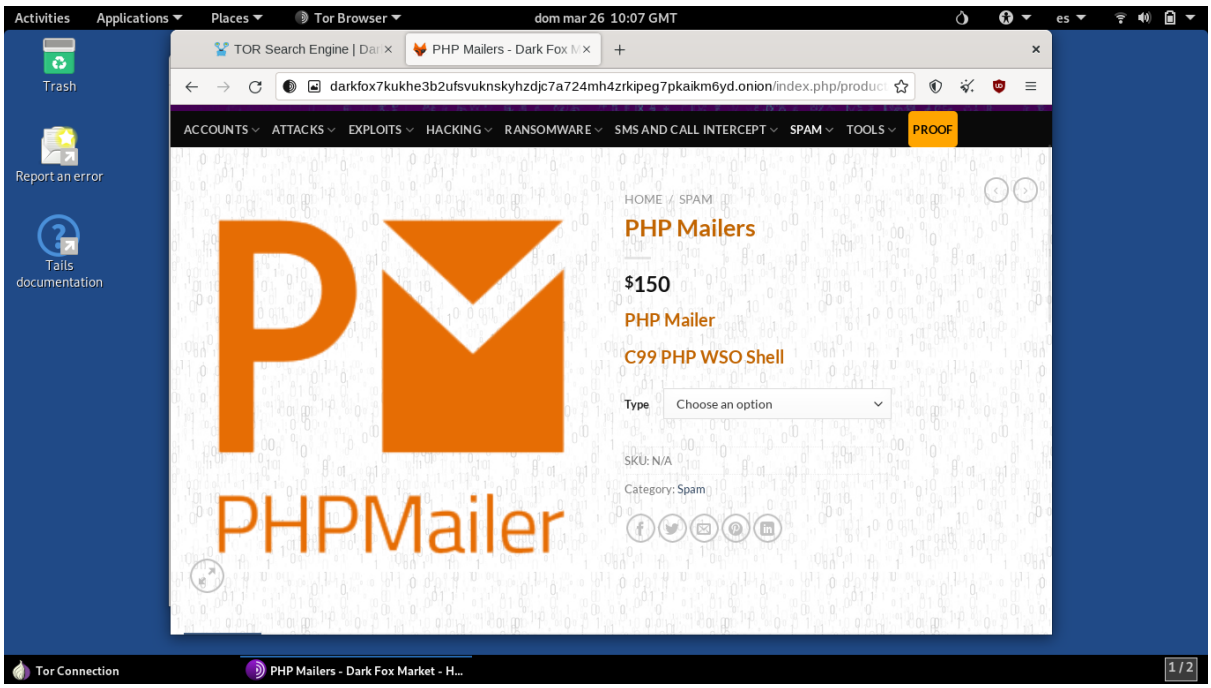

Activities
Applications
Places
Tor Browser
dom mar 26 10:04 GMT
es
Trash
Report an error
Tails documentation
TOR Search Engine | Dar
Search results for ransom
juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/search/?q=ransomware
AHMIA
ransomware as a service
Search
About Ahmia
Statistics
Add Service
i2p search
Contact
Blacklist
Any Time
Omitted very similar entries. Displaying 190 matches in 0.64 seconds. Page 1 of 2 .
Ransomware As a Service - Dark Fox Market - Hacking Service
Now you will pay Ransomware available as a service.Price includes:1 exe file with your payment informationYou will receive the .exe file which
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion — 1 month, 1 week ago —
Ransomware – The Darkweb Marketplace
No description provided
4uasd75w424pn73etyjufvtiqg62csm5nnwk3twfnjhvsw3mkjrp3kad.onion — 4 days, 13 hours ago —
CUSTOM-MADE RANSOMWARE - DarkHidden marketplace - guaranted secure escrow system
CUSTOM-MADE RANSOMWARE Ransomware is a form of malware where person attack victim system with malicious code. Their intent is to lock out of system
762ydpdaq52dcatqyqmqjskgvuqqo6ff7453wqal3dxxgdd5hbzt4zid.onion — 2 weeks, 2 days ago —
CUSTOM-MADE RANSOMWARE | agora road marketplace-verified vendors - secure escrow system
Tor Connection
Search results for ransomware as a...
1 / 2

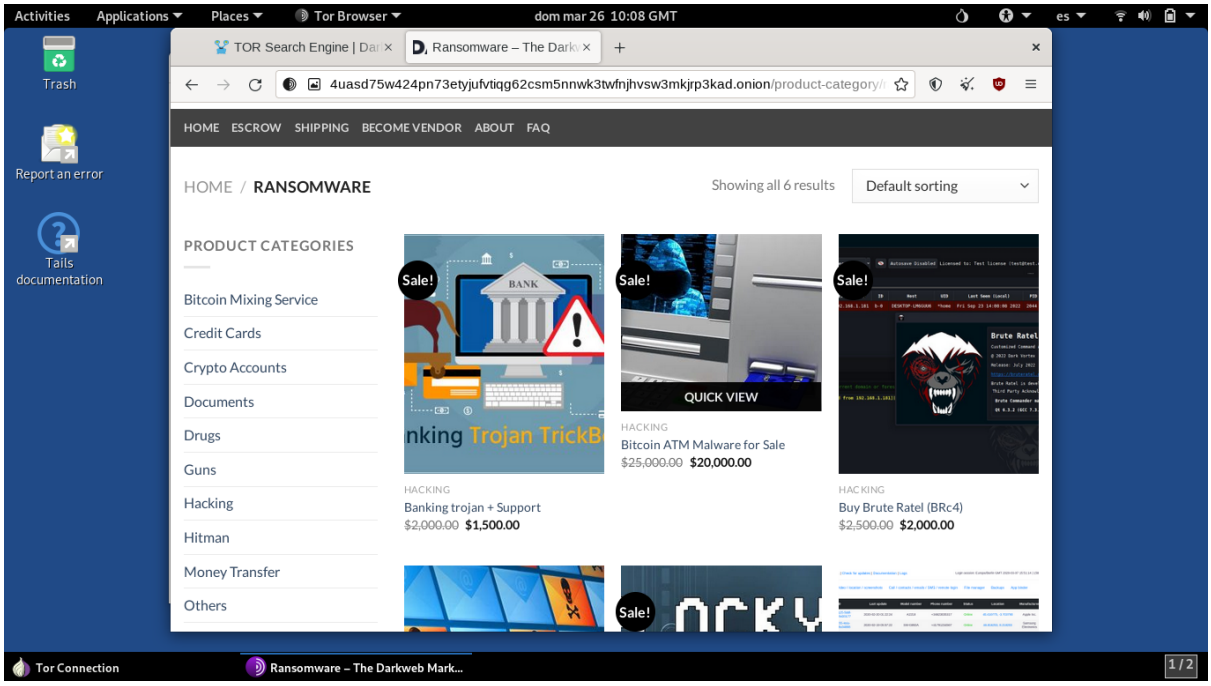

Activities
Applications
Places
Tor Browser
dom mar 26 10:05 GMT
es
Trash
Report an error
Tails documentation
TOR Search Engine | Dar
Take Site Down (DDOS A
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion/index.php/product
EMAIL : darkfox@keemail.me Telegram : https://t.me/darkfoxservices
HOME
CUSTOM ORDER
BUY BITCOIN
DARKFOX
Search...
CART / $0
0
ACCOUNTS
ATTACKS
EXPLOITS
HACKING
RANSOMWARE
SMS AND CALL INTERCEPT
SPAM
TOOLS
PROOF
HOME / ATTACKS
Take Site Down (DDOS Attack)
$260 – $860
A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
Hours
Choose an option
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion/wp-content/uploads/2020/10/www.png
Tor Connection
Take Site Down (DDOS Attack) Dar...
1 / 2

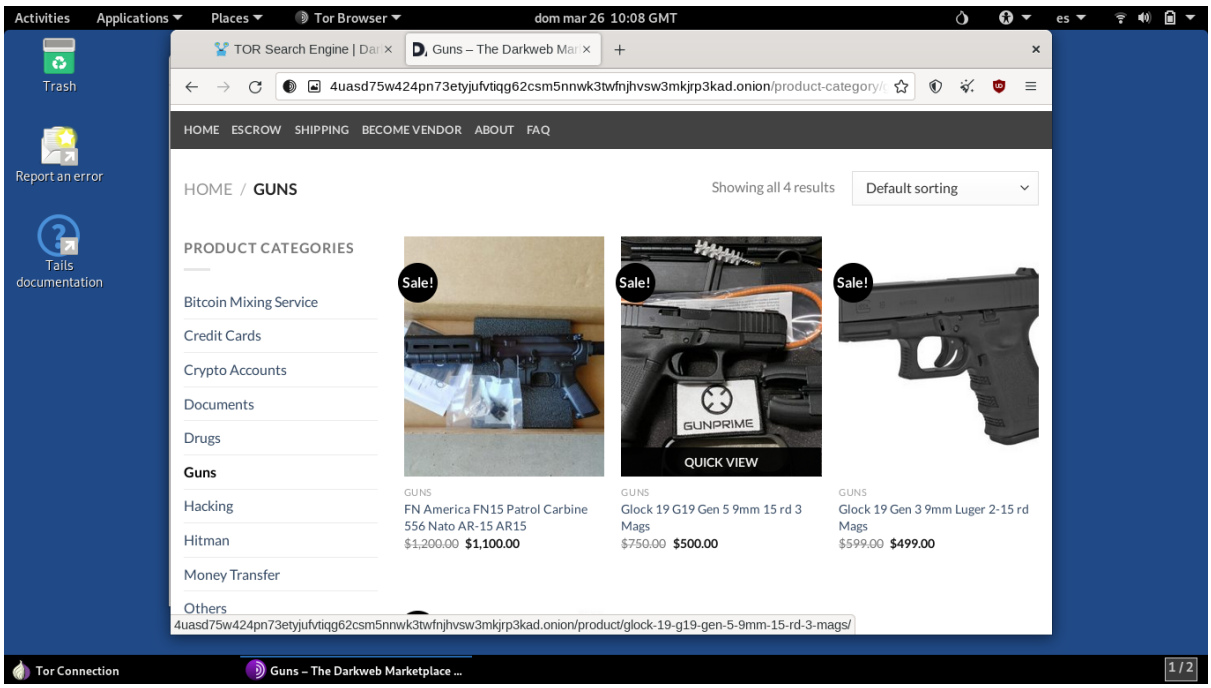

Activities
Applications
Places
Tor Browser
dom mar 26 10:06 GMT
es
Trash
Report an error
Tails documentation
TOR Search Engine | Dar
Visa Card - Dark Fox Mar
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion/index.php/product
ACCOUNTS
ATTACKS
EXPLOITS
HACKING
RANSOMWARE
SMS AND CALL INTERCEPT
SPAM
TOOLS
PROOF
HOME / ACCOUNTS
Visa Card
$120 – $550
Term of validity – 1-2 years
Online Statement
100% Balance Guaranteed
Time to receive: 4-8 hours
0000 0000 0000 0000
VISA
Choose Balance
Choose an option
Card Statement
Choose an option
700-1,000
1,000-1,500
1,500-2,000
2,000-3,000
SKU: N/A
Category: Accounts
Tor Connection
Visa Card - Dark Fox Market - Hack...
1 / 2

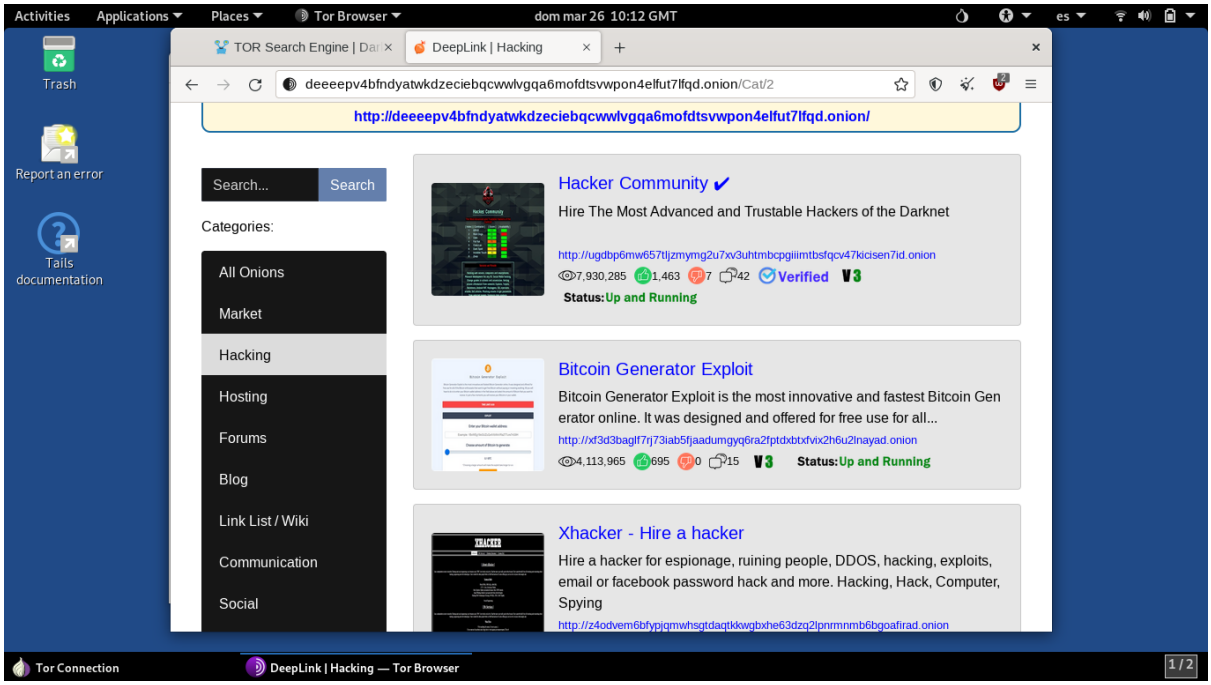

Activities
Applications
Places
Tor Browser
dom mar 26 10:07 GMT
es
Trash
Report an error
Tails documentation
TOR Search Engine | Dar
Visa Card - Dark Fox Mar
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion/index.php/product
DARKFOX
Search...
CART / $0
0
ACCOUNTS
ATTACKS
EXPLOITS
HACKING
RANSOMWARE
SMS AND CALL INTERCEPT
SPAM
TOOLS
PROOF
DESCRIPTION
ADDITIONAL INFORMATION
USA Wells Fargo Bank – 434256 Bin
UK Barclays Bank – 465901 Bin
Canada Royal Bank – 451992 Bin
Denmark Nordea Bank – 402620 Bin
Spain Caixa Bank – 467021 Bin
Cards are valid for 1-2 years. Card balance is in the country currency.
Once you make order open support ticket and mention card country you need in order to receive the full card details.
We can provide the statement for the card as well since we have access to the online banking details. Statement is charged extra as it is a manual operation.
You can choose how many statements you need. If you order the statement option open support ticket and mention for which date you need
Tor Connection
Visa Card - Dark Fox Market - Hack...
1 / 2

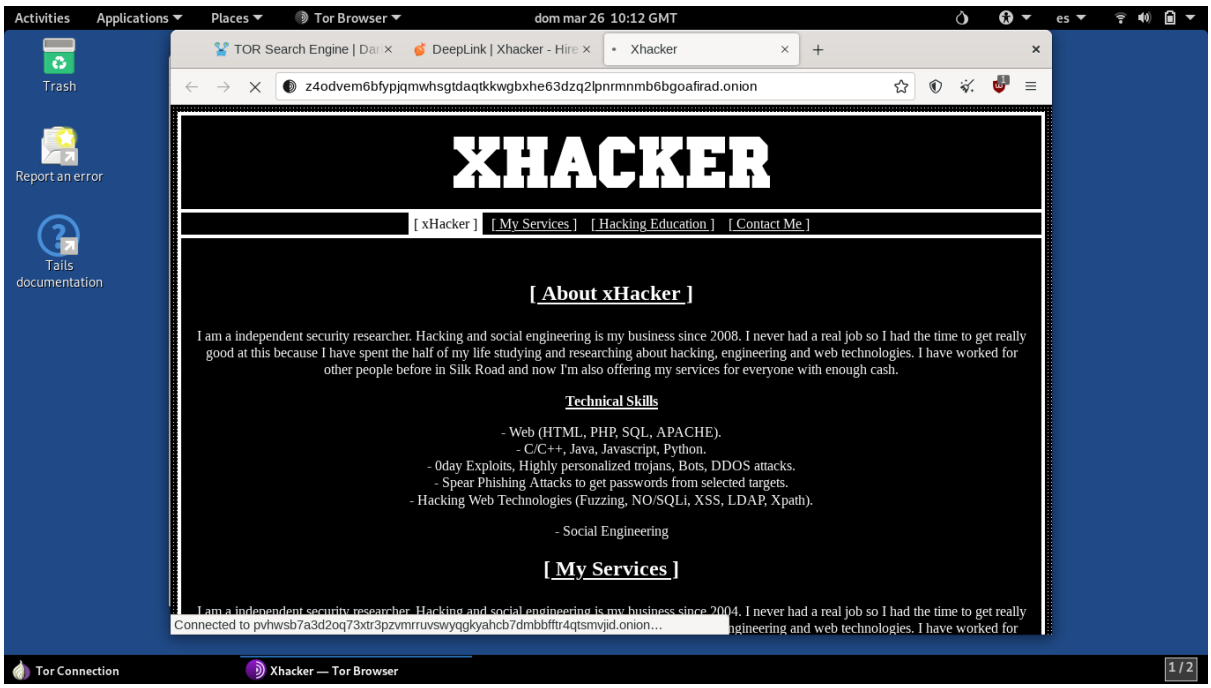

Activities
Applications
Places
Tor Browser
dom mar 26 10:07 GMT
es
TOR Search Engine | Dar
Apple Developer Account
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion/index.php/pro
ACCOUNTS
ATTACKS
EXPLOITS
HACKING
RANSOMWARE
SMS AND CALL INTERCEPT
SPAM
TOOLS
PROOF
Trash
Report an error
Tails documentation
HOME / ACCOUNTS
Apple Developer Account
$250 – $1,000
Each account includes:
Accessible Email account.
App Store ready to publish apps.
Account Type
Choose an option
SKU: N/A
Category: Accounts
Tor Connection
Apple Developer Account Publish ...
1 / 2

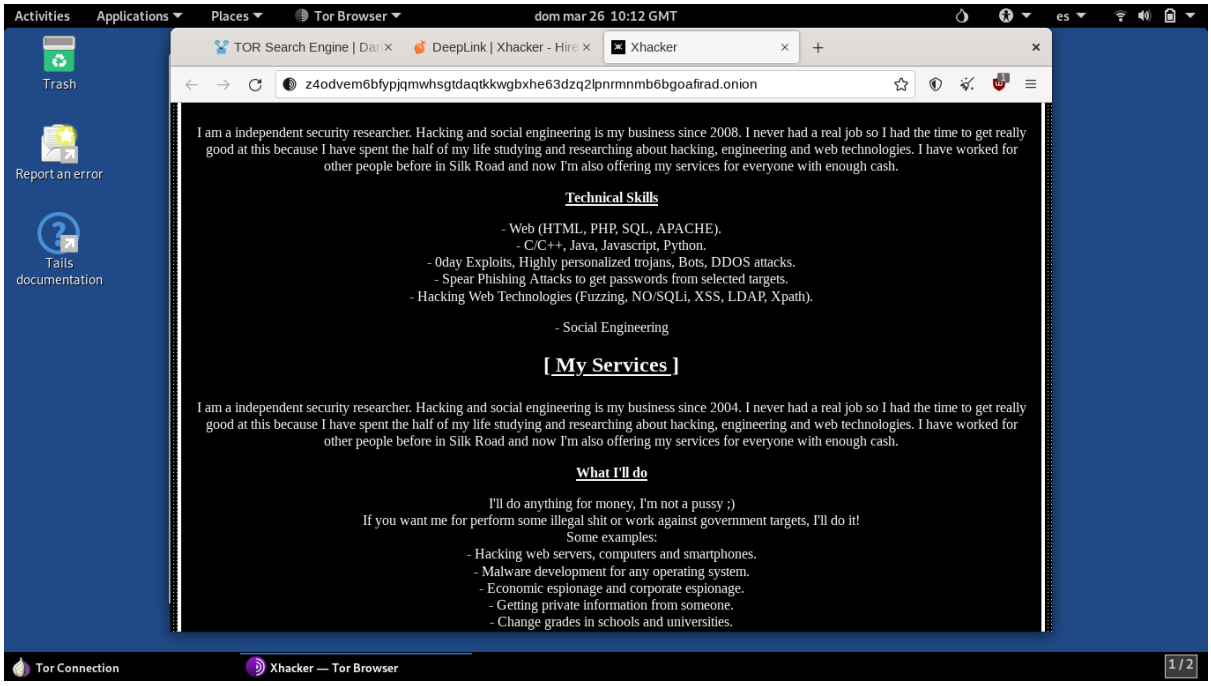

Activities
Applications
Places
Tor Browser
dom mar 26 10:07 GMT
es
TOR Search Engine | Dar
PHP Mailers - Dark Fox M
darkfox7kukhe3b2ufsvuknskyhzdjc7a724mh4zrkipeg7pkaikm6yd.onion/index.php/product
ACCOUNTS
ATTACKS
EXPLOITS
HACKING
RANSOMWARE
SMS AND CALL INTERCEPT
SPAM
TOOLS
PROOF
Trash
Report an error
Tails documentation
HOME / SPAM
PHP Mailers
$150
PHP Mailer
C99 PHP WSO Shell
Type
Choose an option
SKU: N/A
Category: Spam
PHPMailer
Tor Connection
PHP Mailers - Dark Fox Market - H...
1 / 2

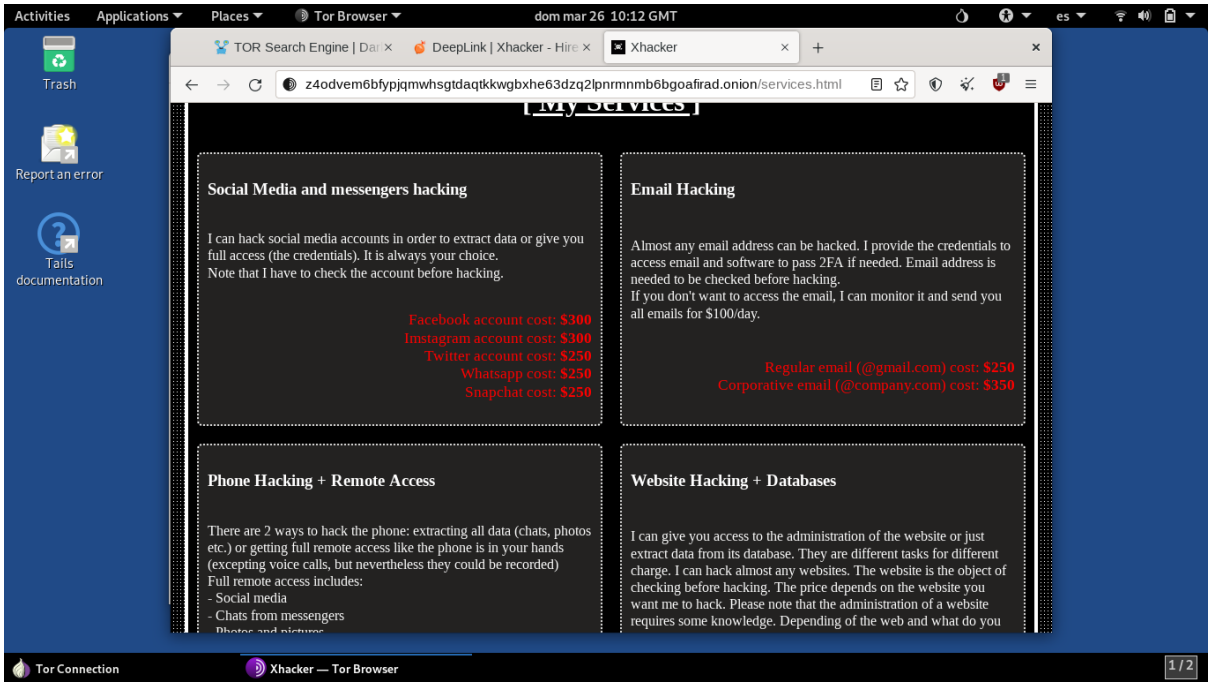

Activities
Applications
Places
Tor Browser
dom mar 26 10:08 GMT
es
Trash
Report an error
Tails documentation
TOR Search Engine | Dar
Ransomware – The Dark
4uasd75w424pn73etyjufvtiqg62csm5nnwk3twfnjhvsw3mkjrp3kad.onion/product-category/r
HOME ESCROW SHIPPING BECOME VENDOR ABOUT FAQ
HOME / RANSOMWARE
Showing all 6 results
Default sorting
PRODUCT CATEGORIES
Bitcoin Mixing Service
Credit Cards
Crypto Accounts
Documents
Drugs
Guns
Hacking
Hitman
Money Transfer
Others
Sale!
QUICK VIEW
HACKING
Bitcoin ATM Malware for Sale
$25,000.00 $20,000.00
HACKING
Banking trojan + Support
$2,000.00 $1,500.00
HACKING
Buy Brute Ratel (BRc4)
$2,500.00 $2,000.00
Tor Connection
Ransomware – The Darkweb Mark...
1 / 2

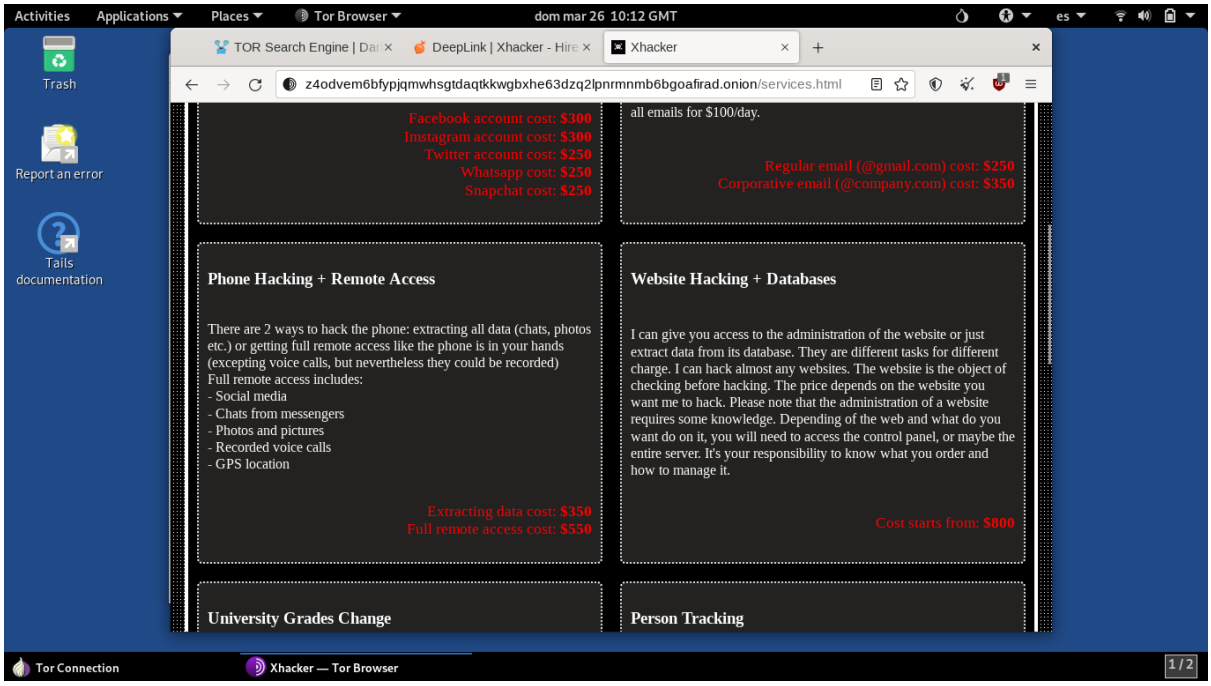

Activities
Applications
Places
Tor Browser
dom mar 26 10:08 GMT
es
Trash
Report an error
Tails documentation
TOR Search Engine | Dar
Guns – The Darkweb Mar
4uasd75w424pn73etyjufvtiqg62csm5nnwk3twfnjhvsw3mkjrp3kad.onion/product-category/r
HOME ESCROW SHIPPING BECOME VENDOR ABOUT FAQ
HOME / GUNS
Showing all 4 results
Default sorting
PRODUCT CATEGORIES
Bitcoin Mixing Service
Credit Cards
Crypto Accounts
Documents
Drugs
Guns
Hacking
Hitman
Money Transfer
Others
Sale!
QUICK VIEW
GUNPRIME
GUNS
FN America FN15 Patrol Carbine 556 Nato AR-15 AR15
$1,200.00 $1,100.00
GUNS
Glock 19 G19 Gen 5 9mm 15 rd 3 Mags
$750.00 $500.00
GUNS
Glock 19 Gen 3 9mm Luger 2-15 rd Mags
$599.00 $499.00
4uasd75w424pn73etyjufvtiqg62csm5nnwk3twfnjhvsw3mkjrp3kad.onion/product/glock-19-g19-gen-5-9mm-15-rd-3-mags/
Tor Connection
Guns – The Darkweb Marketplace ...
1 / 2

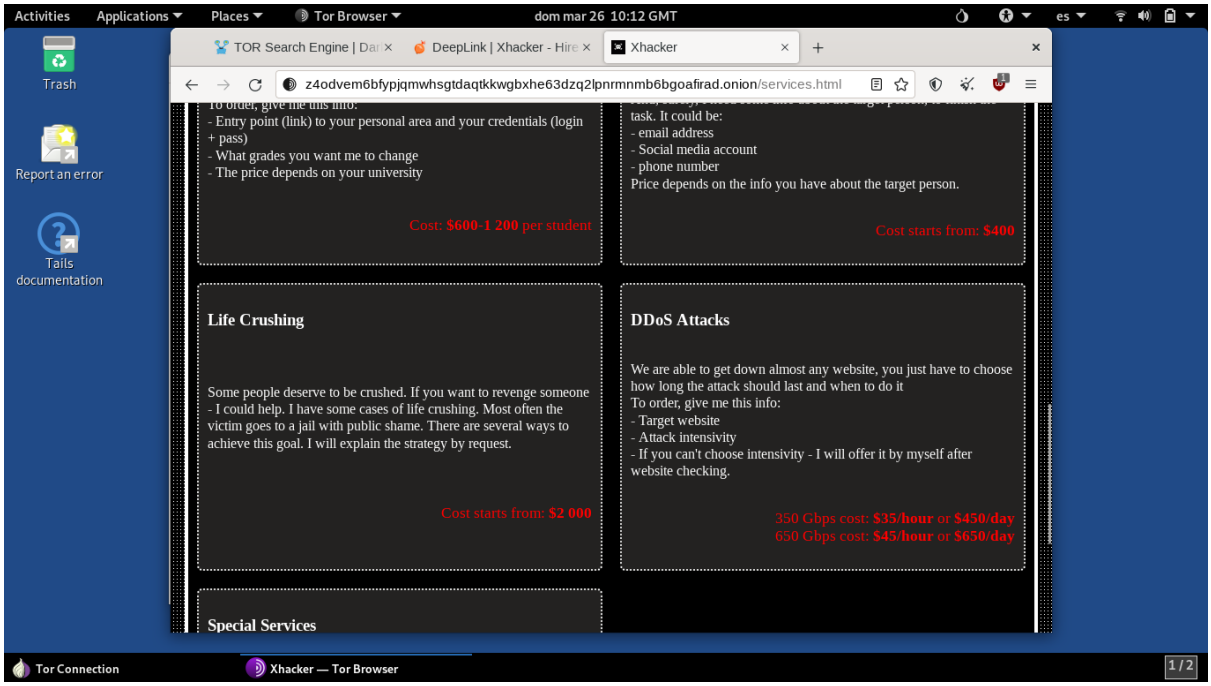

Activities
Applications
Places
Tor Browser
dom mar 26 10:12 GMT
es
TOR Search Engine | Dar
DeepLink | Hacking
deeeepv4bfndyatwkdzeciebqcwwlvgqa6mofdtsvwpon4elfut7lfqd.onion/Cat/2
http://deeeepv4bfndyatwkdzeciebqcwwlvgqa6mofdtsvwpon4elfut7lfqd.onion/
Trash
Report an error
Tails documentation
Search...
Search
Categories:
All Onions
Market
Hacking
Hosting
Forums
Blog
Link List / Wiki
Communication
Social
Hacker Community ✔
Hire The Most Advanced and Trustable Hackers of the Darknet
http://ugdbp6mw657tljzmymg2u7xv3uhtmbcpgiiimtbsfqcv47kicisen7id.onion
7,930,285 1,463 7 42 Verified V3
Status: Up and Running
Bitcoin Generator Exploit
Bitcoin Generator Exploit is the most innovative and fastest Bitcoin Gen erator online. It was designed and offered for free use for all...
http://xf3d3baglf7rj73iab5fjaadumgyq6ra2fptdxbtxfvix2h6u2lnayad.onion
4,113,965 695 0 15 V3 Status: Up and Running
Xhacker - Hire a hacker
Hire a hacker for espionage, ruining people, DDOS, hacking, exploits, email or facebook password hack and more. Hacking, Hack, Computer, Spying
http://z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion
Tor Connection
DeepLink | Hacking — Tor Browser
1 / 2

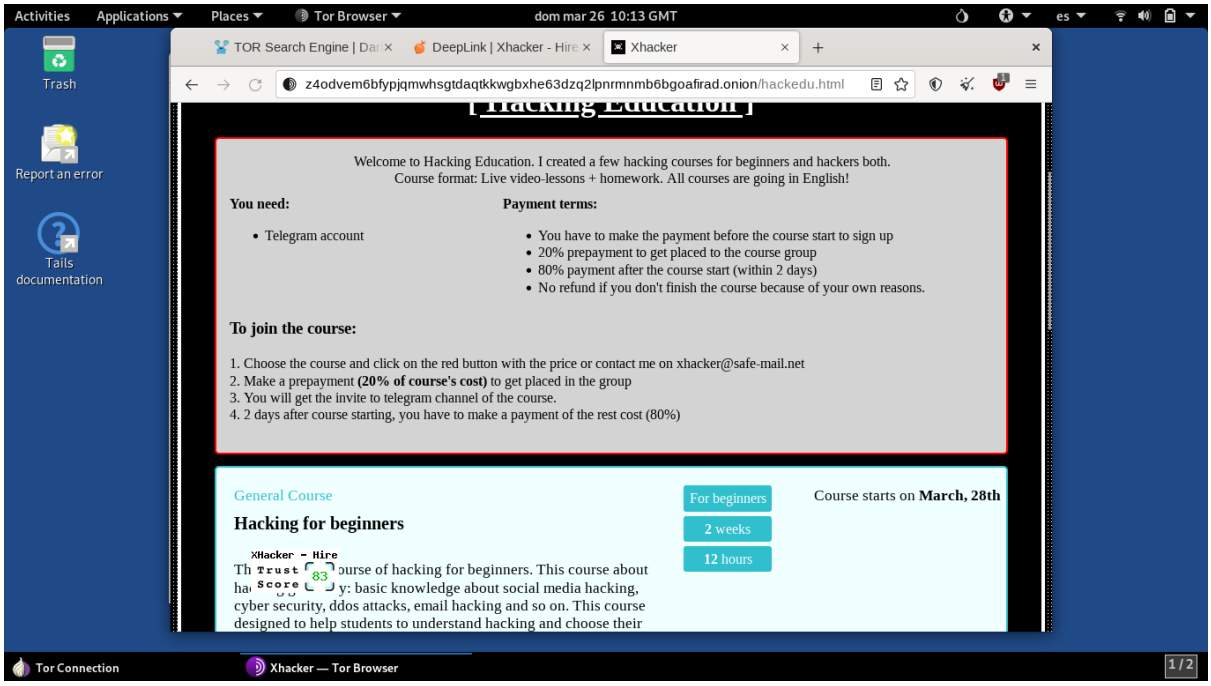

Activities
Applications
Places
Tor Browser
dom mar 26 10:12 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion
Trash
Report an error
Tails documentation
XHACKER
[xHacker] [My Services] [Hacking Education] [Contact Me]
[About xHacker]
I am a independent security researcher. Hacking and social engineering is my business since 2008. I never had a real job so I had the time to get really good at this because I have spent the half of my life studying and researching about hacking, engineering and web technologies. I have worked for other people before in Silk Road and now I'm also offering my services for everyone with enough cash.
Technical Skills
- Web (HTML, PHP, SQL, APACHE).
- C/C++, Java, Javascript, Python.
- 0day Exploits, Highly personalized trojans, Bots, DDOS attacks.
- Spear Phishing Attacks to get passwords from selected targets.
- Hacking Web Technologies (Fuzzing, NO/SQLi, XSS, LDAP, Xpath).
- Social Engineering
[My Services]
I am a independent security researcher. Hacking and social engineering is my business since 2004. I never had a real job so I had the time to get really
Connected to pvhwsb7a3d2oq73xtr3pzvmrruvswyqgkyahcb7dmbbfftr4qtsmvjid.onion…
ngineering and web technologies. I have worked for
Tor Connection
Xhacker — Tor Browser
1 / 2

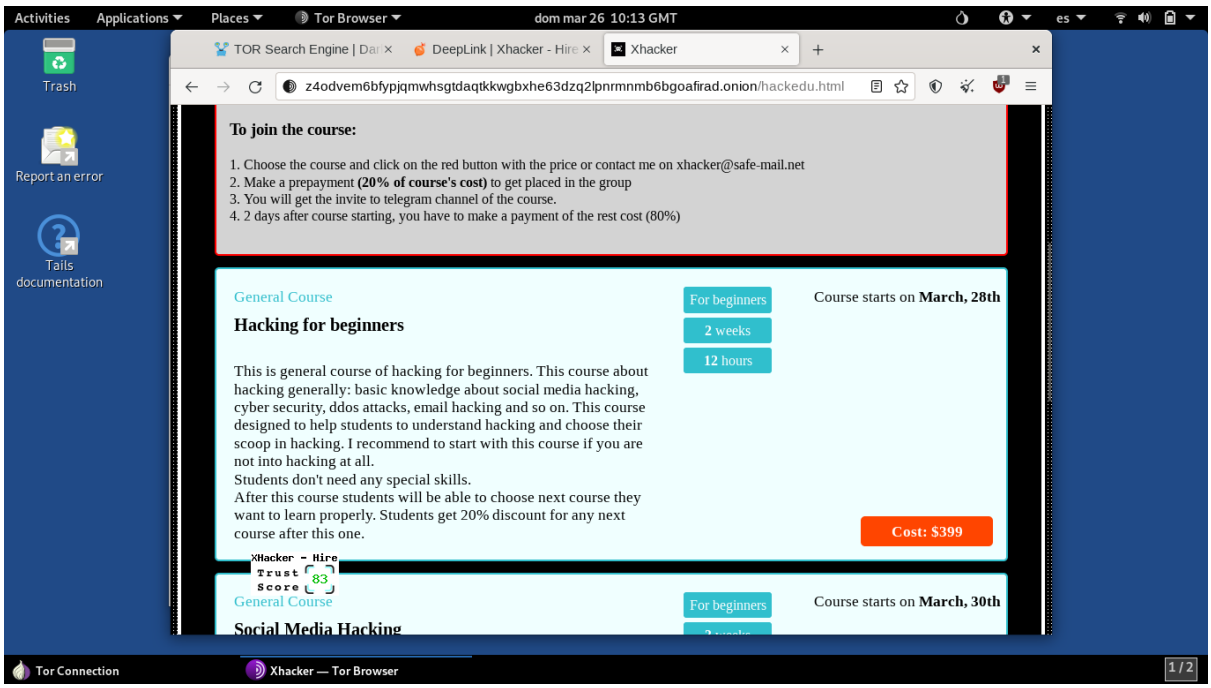

Activities
Applications
Places
Tor Browser
dom mar 26 10:12 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion
Trash
Report an error
Tails documentation
I am a independent security researcher. Hacking and social engineering is my business since 2008. I never had a real job so I had the time to get really good at this because I have spent the half of my life studying and researching about hacking, engineering and web technologies. I have worked for other people before in Silk Road and now I'm also offering my services for everyone with enough cash.
Technical Skills
- Web (HTML, PHP, SQL, APACHE).
- C/C++, Java, Javascript, Python.
- 0day Exploits, Highly personalized trojans, Bots, DDOS attacks.
- Spear Phishing Attacks to get passwords from selected targets.
- Hacking Web Technologies (Fuzzing, NO/SQLi, XSS, LDAP, Xpath).
- Social Engineering
[My Services]
I am a independent security researcher. Hacking and social engineering is my business since 2004. I never had a real job so I had the time to get really good at this because I have spent the half of my life studying and researching about hacking, engineering and web technologies. I have worked for other people before in Silk Road and now I'm also offering my services for everyone with enough cash.
What I'll do
I'll do anything for money, I'm not a pussy ;)
If you want me for perform some illegal shit or work against government targets, I'll do it!
Some examples:
- Hacking web servers, computers and smartphones.
- Malware development for any operating system.
- Economic espionage and corporate espionage.
- Getting private information from someone.
- Change grades in schools and universities.
Tor Connection
Xhacker — Tor Browser
1 / 2

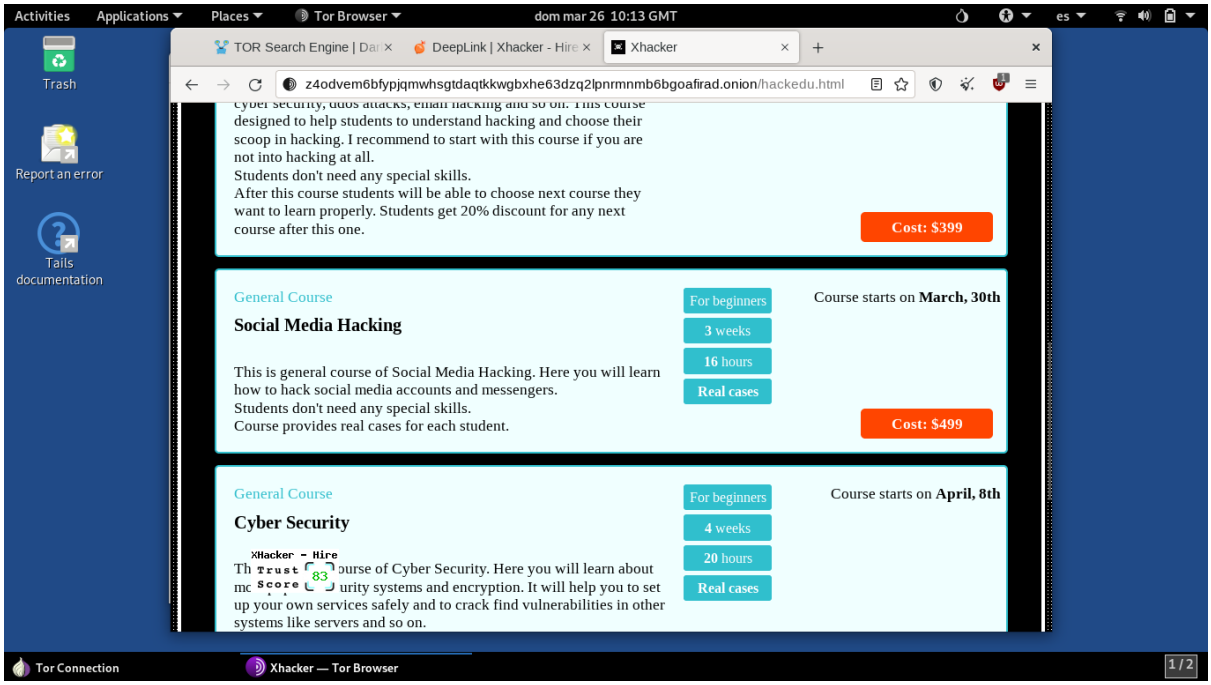

Activities
Applications
Places
Tor Browser
dom mar 26 10:12 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/services.html
Trash
Report an error
Tails documentation
Social Media and messengers hacking
I can hack social media accounts in order to extract data or give you full access (the credentials). It is always your choice.
Note that I have to check the account before hacking.
Facebook account cost: $300
Instagram account cost: $300
Twitter account cost: $250
Whatsapp cost: $250
Snapchat cost: $250
Email Hacking
Almost any email address can be hacked. I provide the credentials to access email and software to pass 2FA if needed. Email address is needed to be checked before hacking.
If you don't want to access the email, I can monitor it and send you all emails for $100/day.
Regular email (@gmail.com) cost: $250
Corporative email (@company.com) cost: $350
Phone Hacking + Remote Access
There are 2 ways to hack the phone: extracting all data (chats, photos etc.) or getting full remote access like the phone is in your hands (excepting voice calls, but nevertheless they could be recorded)
Full remote access includes:
- Social media
- Chats from messengers
Website Hacking + Databases
I can give you access to the administration of the website or just extract data from its database. They are different tasks for different charge. I can hack almost any websites. The website is the object of checking before hacking. The price depends on the website you want me to hack. Please note that the administration of a website requires some knowledge. Depending of the web and what do you
Tor Connection
Xhacker — Tor Browser
1 / 2

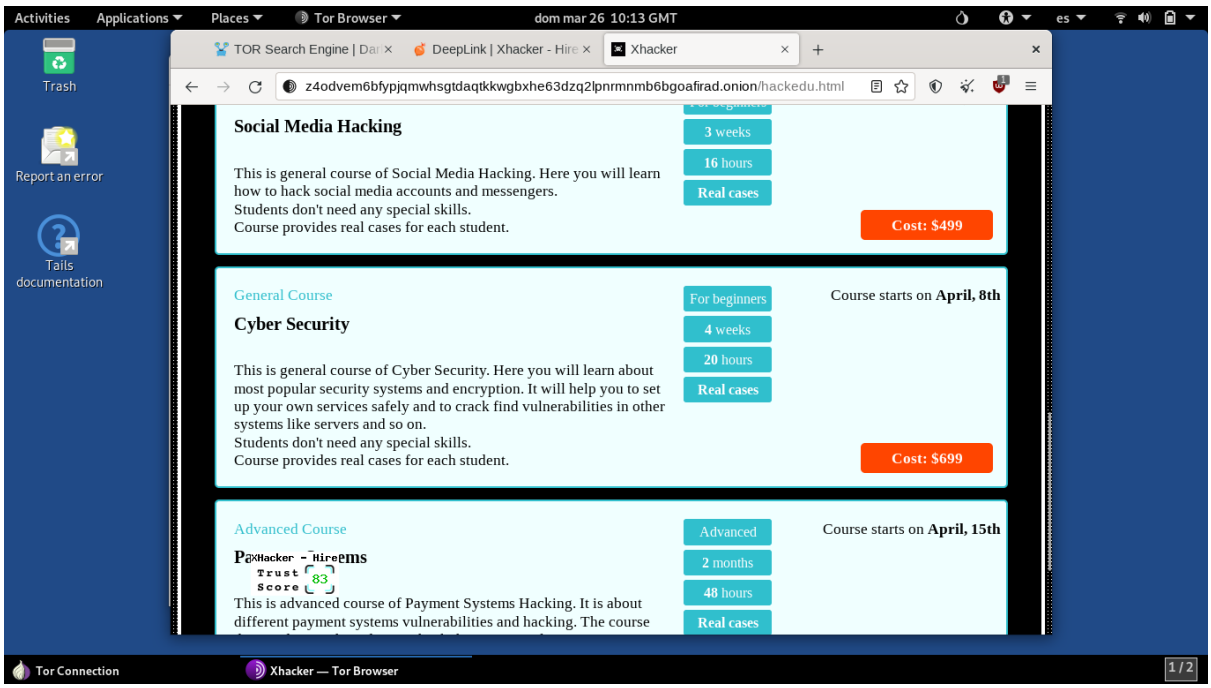

Activities
Applications
Places
Tor Browser
dom mar 26 10:12 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/services.html
Trash
Report an error
Tails documentation
Facebook account cost: $300
Imstagram account cost: $300
Twitter account cost: $250
Whatsapp cost: $250
Snapchat cost: $250
all emails for $100/day.
Regular email (@gmail.com) cost: $250
Corporative email (@company.com) cost: $350
Phone Hacking + Remote Access
There are 2 ways to hack the phone: extracting all data (chats, photos etc.) or getting full remote access like the phone is in your hands (excepting voice calls, but nevertheless they could be recorded)
Full remote access includes:
- Social media
- Chats from messengers
- Photos and pictures
- Recorded voice calls
- GPS location
Extracting data cost: $350
Full remote access cost: $550
Website Hacking + Databases
I can give you access to the administration of the website or just extract data from its database. They are different tasks for different charge. I can hack almost any websites. The website is the object of checking before hacking. The price depends on the website you want me to hack. Please note that the administration of a website requires some knowledge. Depending of the web and what do you want do on it, you will need to access the control panel, or maybe the entire server. It's your responsibility to know what you order and how to manage it.
Cost starts from: $800
University Grades Change
Person Tracking
Tor Connection
Xhacker — Tor Browser
1 / 2

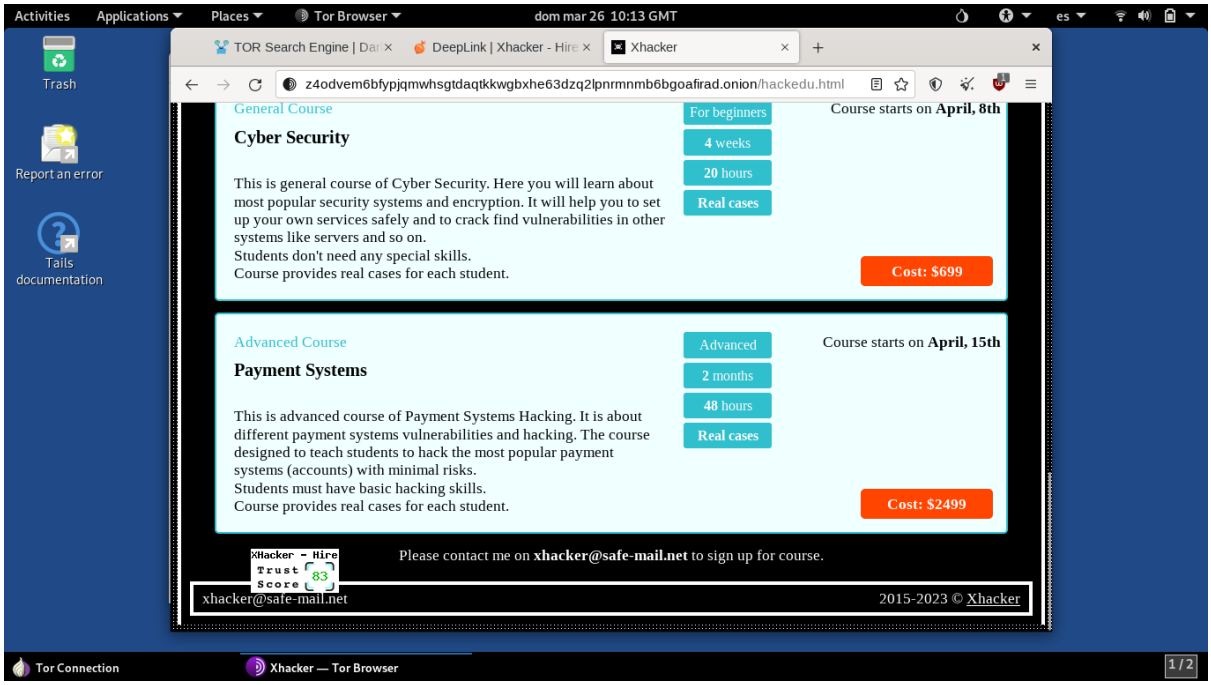

Activities
Applications
Places
Tor Browser
dom mar 26 10:12 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/services.html
Trash
Report an error
Tails documentation
- Entry point (link) to your personal area and your credentials (login + pass)
- What grades you want me to change
- The price depends on your university
Cost: $600-1 200 per student
task. It could be:
- email address
- Social media account
- phone number
Price depends on the info you have about the target person.
Cost starts from: $400
Life Crushing
Some people deserve to be crushed. If you want to revenge someone - I could help. I have some cases of life crushing. Most often the victim goes to a jail with public shame. There are several ways to achieve this goal. I will explain the strategy by request.
Cost starts from: $2 000
DDoS Attacks
We are able to get down almost any website, you just have to choose how long the attack should last and when to do it
To order, give me this info:
- Target website
- Attack intensivity
- If you can't choose intensivity - I will offer it by myself after website checking.
350 Gbps cost: $35/hour or $450/day
650 Gbps cost: $45/hour or $650/day
Special Services
Tor Connection
Xhacker — Tor Browser
1 / 2

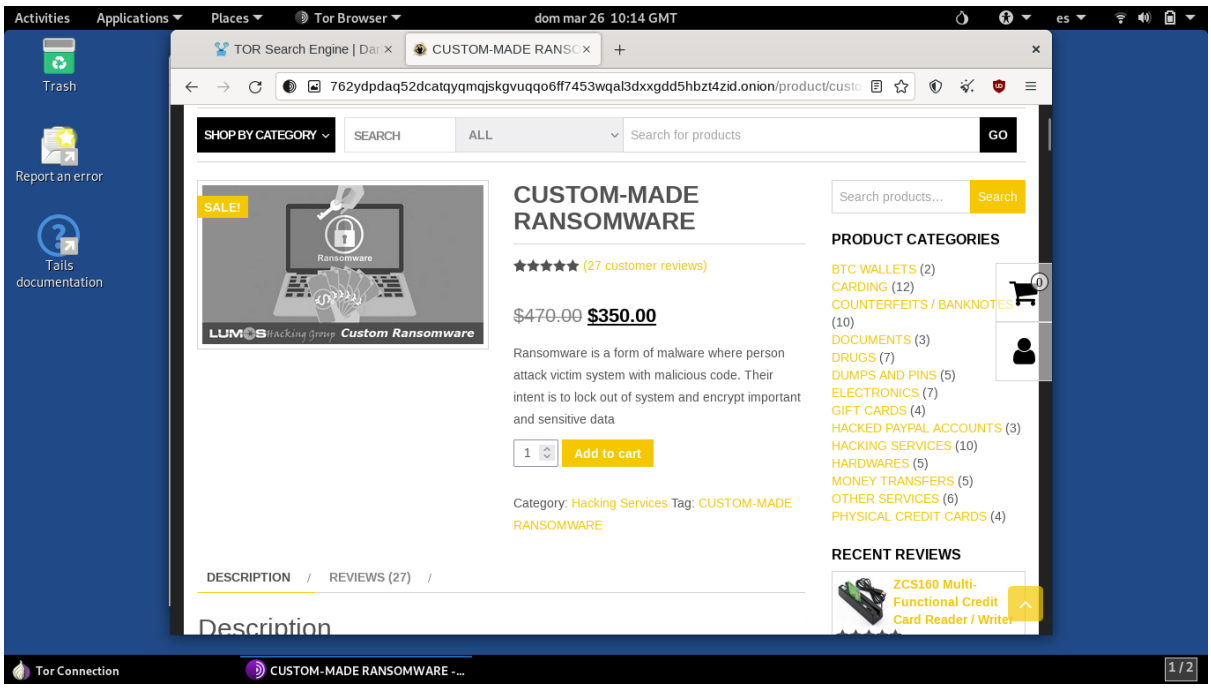

Activities
Applications
Places
Tor Browser
dom mar 26 10:13 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/hackedu.html
Trash
Report an error
Tails documentation
[Hacking Education]
Welcome to Hacking Education. I created a few hacking courses for beginners and hackers both.
Course format: Live video-lessons + homework. All courses are going in English!
You need:
Telegram account
Payment terms:
You have to make the payment before the course start to sign up
20% prepayment to get placed to the course group
80% payment after the course start (within 2 days)
No refund if you don't finish the course because of your own reasons.
To join the course:
1. Choose the course and click on the red button with the price or contact me on xhacker@safe-mail.net
2. Make a prepayment (20% of course's cost) to get placed in the group
3. You will get the invite to telegram channel of the course.
4. 2 days after course starting, you have to make a payment of the rest cost (80%)
General Course
Hacking for beginners
For beginners
2 weeks
12 hours
Course starts on March, 28th
XHacker - Hire
Trust Score 83
Tor Connection
Xhacker — Tor Browser
1 / 2

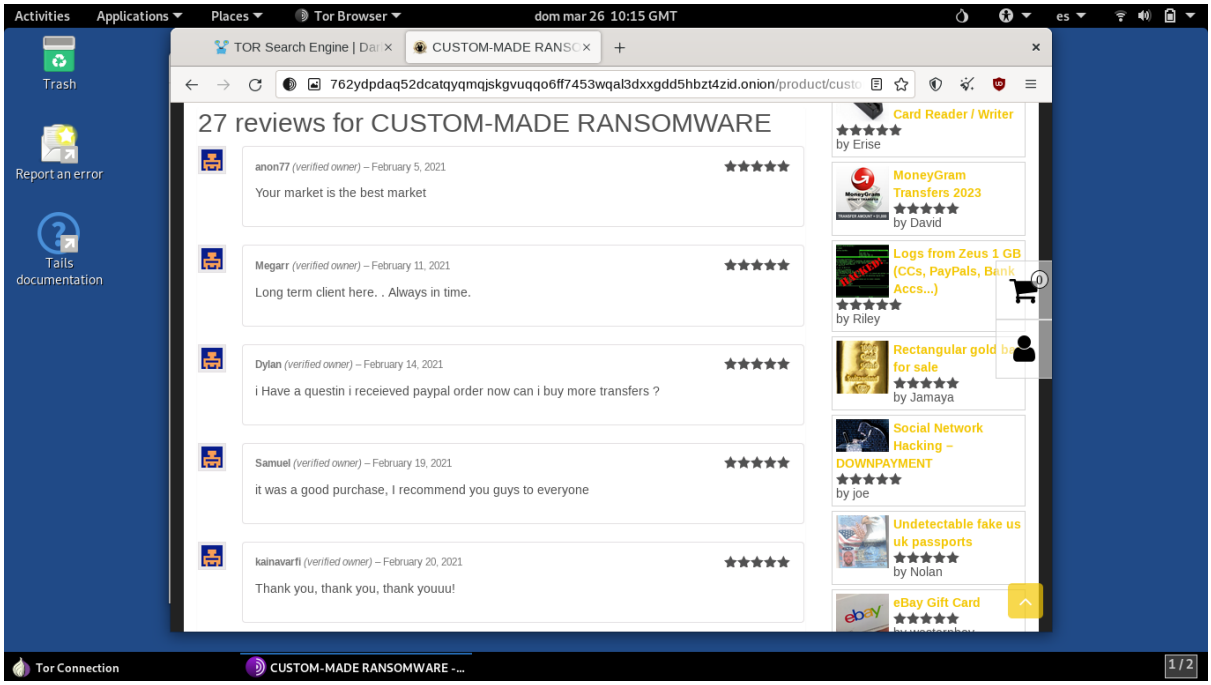

Activities
Applications
Places
Tor Browser
dom mar 26 10:13 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/hackedu.html
Trash
Report an error
Tails documentation
To join the course:
1. Choose the course and click on the red button with the price or contact me on xhacker@safe-mail.net
2. Make a prepayment (20% of course's cost) to get placed in the group
3. You will get the invite to telegram channel of the course.
4. 2 days after course starting, you have to make a payment of the rest cost (80%)
General Course
Hacking for beginners
For beginners
2 weeks
12 hours
Course starts on March, 28th
This is general course of hacking for beginners. This course about hacking generally: basic knowledge about social media hacking, cyber security, ddos attacks, email hacking and so on. This course designed to help students to understand hacking and choose their scoop in hacking. I recommend to start with this course if you are not into hacking at all.
Students don't need any special skills.
After this course students will be able to choose next course they want to learn properly. Students get 20% discount for any next course after this one.
Cost: $399
XHacker - Hire
Trust Score 83
General Course
Social Media Hacking
For beginners
Course starts on March, 30th
Tor Connection
Xhacker — Tor Browser
1 / 2

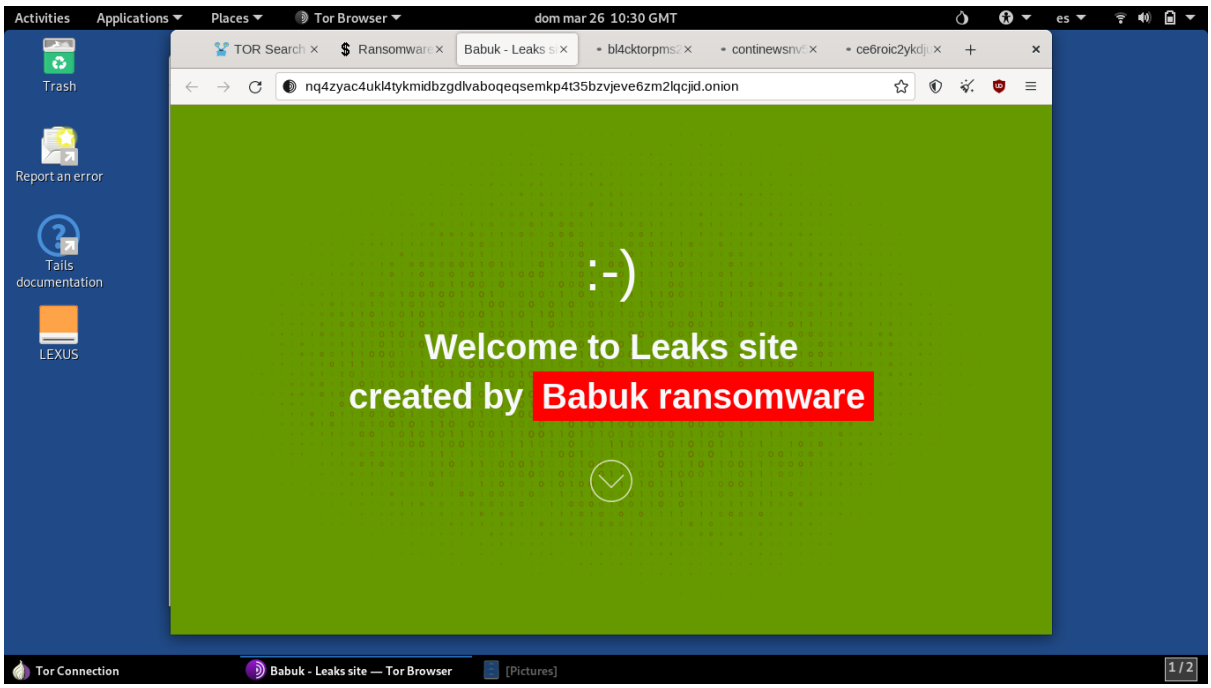

Activities
Applications
Places
Tor Browser
dom mar 26 10:13 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/hackedu.html
Trash
Report an error
Tails documentation
designed to help students to understand hacking and choose their scoop in hacking. I recommend to start with this course if you are not into hacking at all.
Students don't need any special skills.
After this course students will be able to choose next course they want to learn properly. Students get 20% discount for any next course after this one.
Cost: $399
General Course
Social Media Hacking
For beginners
3 weeks
16 hours
Real cases
Course starts on March, 30th
This is general course of Social Media Hacking. Here you will learn how to hack social media accounts and messengers.
Students don't need any special skills.
Course provides real cases for each student.
Cost: $499
General Course
Cyber Security
For beginners
4 weeks
20 hours
Real cases
Course starts on April, 8th
XHacker - Hire
Trust Score 83
Tor Connection
Xhacker — Tor Browser
1 / 2

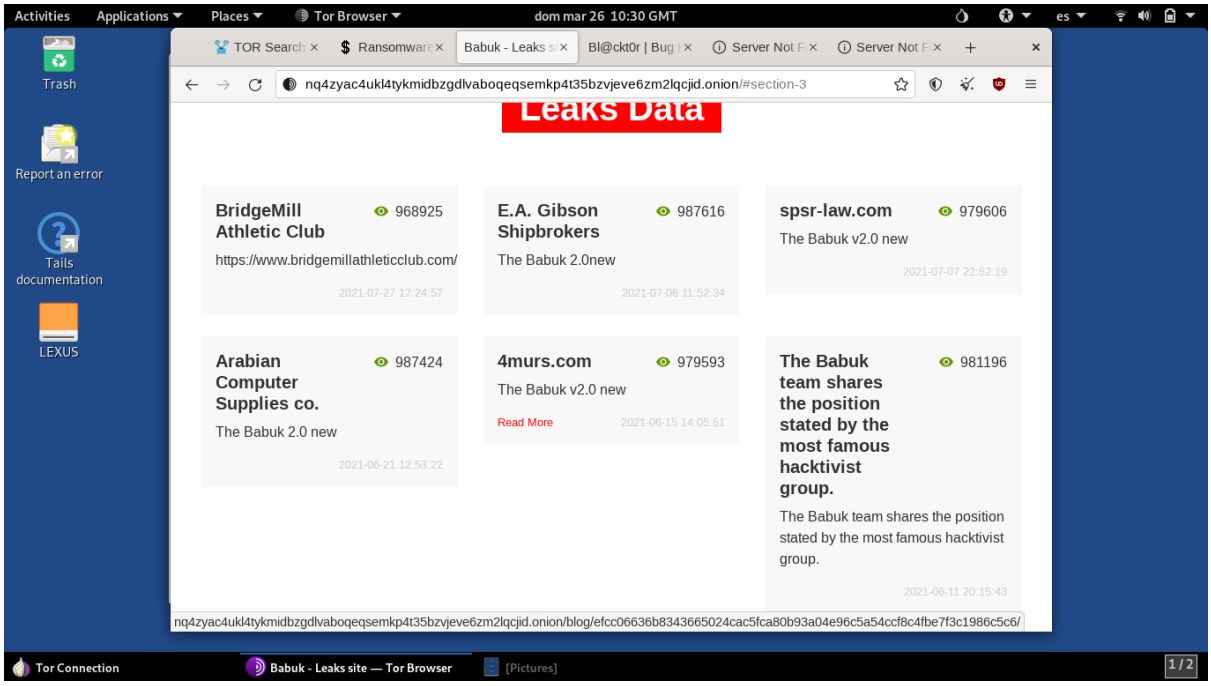

Activities
Applications
Places
Tor Browser
dom mar 26 10:13 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/hackedu.html
Trash
Report an error
Tails documentation
Social Media Hacking
3 weeks
16 hours
Real cases
This is general course of Social Media Hacking. Here you will learn how to hack social media accounts and messengers.
Students don't need any special skills.
Course provides real cases for each student.
Cost: $499
General Course
Cyber Security
For beginners
4 weeks
20 hours
Real cases
Course starts on April, 8th
This is general course of Cyber Security. Here you will learn about most popular security systems and encryption. It will help you to set up your own services safely and to crack find vulnerabilities in other systems like servers and so on.
Students don't need any special skills.
Course provides real cases for each student.
Cost: $699
Advanced Course
Advanced
2 months
48 hours
Real cases
Course starts on April, 15th
XHacker - Hire
Trust Score 83
This is advanced course of Payment Systems Hacking. It is about different payment systems vulnerabilities and hacking. The course
Tor Connection
Xhacker — Tor Browser
1 / 2


Activities
Applications
Places
Tor Browser
dom mar 26 10:13 GMT
es
TOR Search Engine | Dar
DeepLink | Xhacker - Hire
Xhacker
z4odvem6bfypjqmwhsgtdaqtkkwgbxhe63dzq2lpnrmnmb6bgoafirad.onion/hackedu.html
Trash
Report an error
Tails documentation
General Course
Cyber Security
This is general course of Cyber Security. Here you will learn about most popular security systems and encryption. It will help you to set up your own services safely and to crack find vulnerabilities in other systems like servers and so on.
Students don't need any special skills.
Course provides real cases for each student.
For beginners
4 weeks
20 hours
Real cases
Course starts on April, 8th
Cost: $699
Advanced Course
Payment Systems
This is advanced course of Payment Systems Hacking. It is about different payment systems vulnerabilities and hacking. The course designed to teach students to hack the most popular payment systems (accounts) with minimal risks.
Students must have basic hacking skills.
Course provides real cases for each student.
Advanced
2 months
48 hours
Real cases
Course starts on April, 15th
Cost: $2499
XHacker - Hire
Trust Score 83
Please contact me on xhacker@safe-mail.net to sign up for course.
xhacker@safe-mail.net
2015-2023 © Xhacker
Tor Connection
Xhacker — Tor Browser
1 / 2

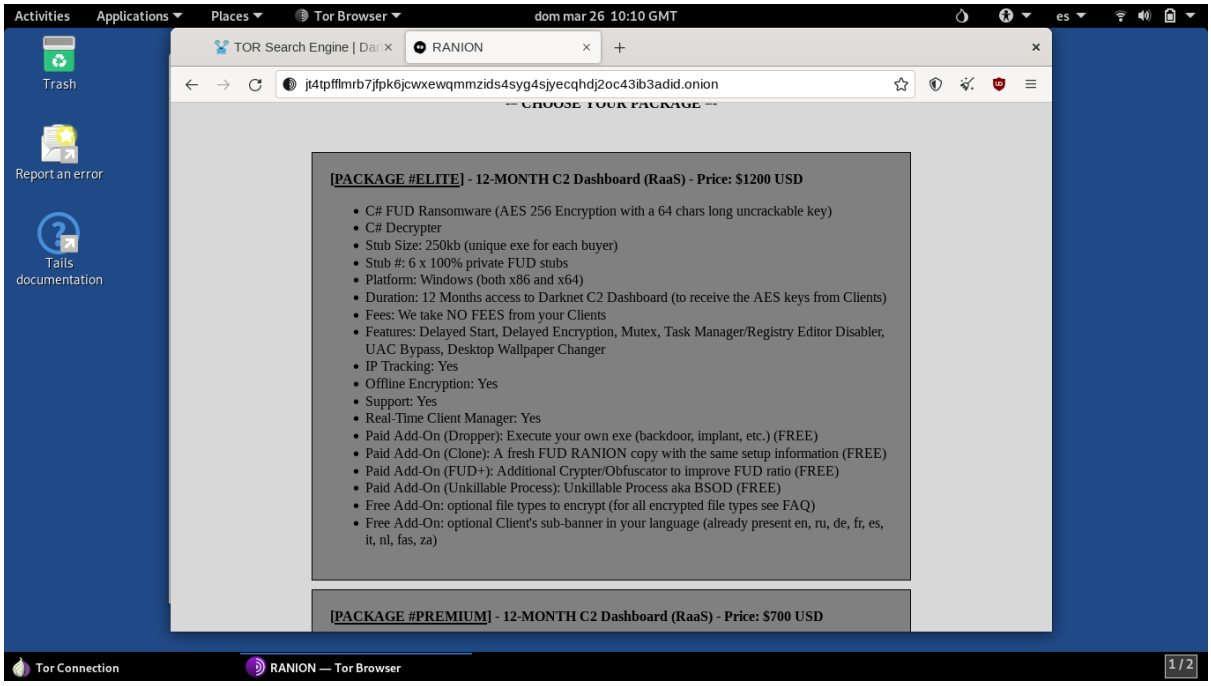

Activities
Applications
Places
Tor Browser
dom mar 26 10:14 GMT
es
TOR Search Engine | Dar
CUSTOM-MADE RANSC
762ydpdaq52dcatqyqmqjskgvuqqo6ff7453wqal3dxxgdd5hbzt4zid.onion/product/custo
Trash
Report an error
Tails documentation
SHOP BY CATEGORY
SEARCH
ALL
Search for products
GO
SALE!
Ransomware
LUMOS Hacking Group Custom Ransomware
CUSTOM-MADE RANSOMWARE
(27 customer reviews)
$470.00 $350.00
Ransomware is a form of malware where person attack victim system with malicious code. Their intent is to lock out of system and encrypt important and sensitive data
1
Add to cart
Category: Hacking Services Tag: CUSTOM-MADE RANSOMWARE
Search products…
Search
PRODUCT CATEGORIES
BTC WALLETS (2)
CARDING (12)
COUNTERFEITS / BANKNOTES (10)
DOCUMENTS (3)
DRUGS (7)
DUMPS AND PINS (5)
ELECTRONICS (7)
GIFT CARDS (4)
HACKED PAYPAL ACCOUNTS (3)
HACKING SERVICES (10)
HARDWARES (5)
MONEY TRANSFERS (5)
OTHER SERVICES (6)
PHYSICAL CREDIT CARDS (4)
RECENT REVIEWS
ZCS160 Multi-Functional Credit Card Reader / Writer
DESCRIPTION
REVIEWS (27)
Description
Tor Connection
CUSTOM-MADE RANSOMWARE -...
1 / 2

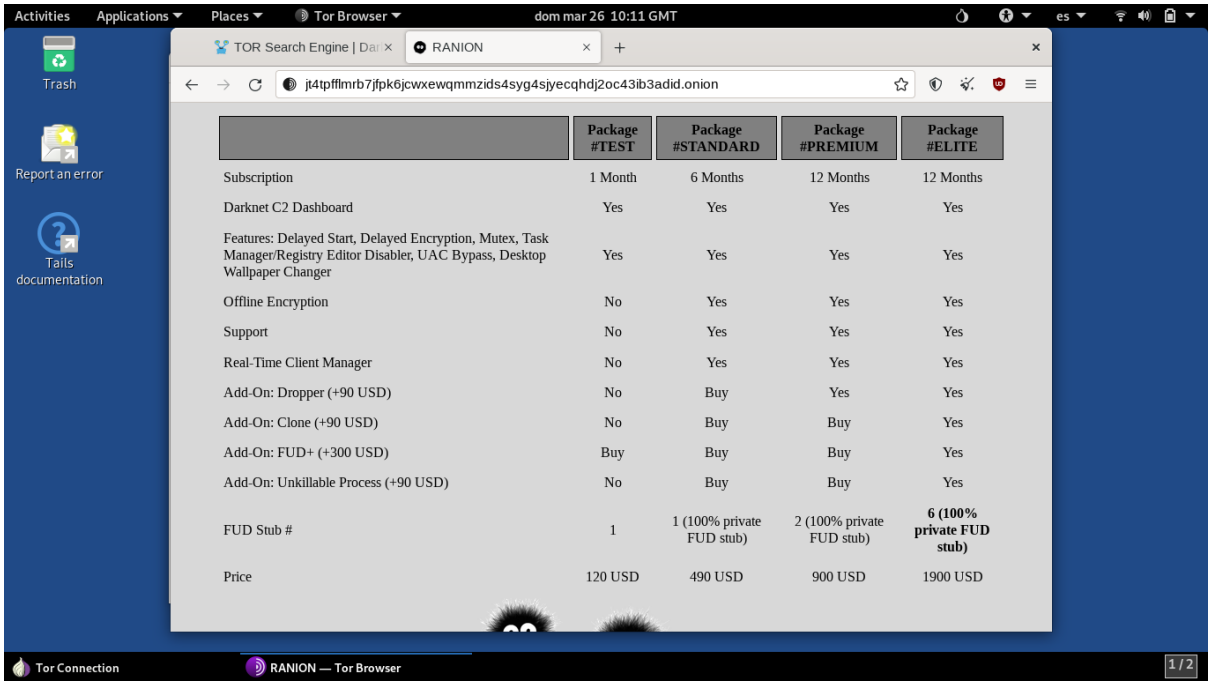

Activities
Applications
Places
Tor Browser
dom mar 26 10:15 GMT
es
TOR Search Engine | Dar
CUSTOM-MADE RANSC
762ydpdaq52dcatqyqmqjskgvuqqo6ff7453wqal3dxxgdd5hbzt4zid.onion/product/custo
Trash
Report an error
Tails documentation
27 reviews for CUSTOM-MADE RANSOMWARE
anon77 (verified owner) – February 5, 2021
Your market is the best market
Megarr (verified owner) – February 11, 2021
Long term client here. . Always in time.
Dylan (verified owner) – February 14, 2021
i Have a questin i receieved paypal order now can i buy more transfers ?
Samuel (verified owner) – February 19, 2021
it was a good purchase, I recommend you guys to everyone
kainavarfi (verified owner) – February 20, 2021
Thank you, thank you, thank youuu!
Card Reader / Writer
by Erise
MoneyGram Transfers 2023
by David
Logs from Zeus 1 GB (CCs, PayPals, Bank Accs...)
by Riley
Rectangular gold b for sale
by Jamaya
Social Network Hacking – DOWNPAYMENT
by joe
Undetectable fake us uk passports
by Nolan
eBay Gift Card
Tor Connection
CUSTOM-MADE RANSOMWARE -...
1 / 2


Activities
Applications
Places
Tor Browser
dom mar 26 10:30 GMT
es
TOR Search
Ransomware
Babuk - Leaks s
bl4cktorpms
continewsnv
ce6roic2ykdj
nq4zyac4ukl4tykmidbzgdlvaboqeqsemkp4t35bzvjeve6zm2lqcjid.onion
Trash
Report an error
Tails documentation
LEXUS
:-)
Welcome to Leaks site
created by Babuk ransomware
Tor Connection
Babuk - Leaks site — Tor Browser
[Pictures]
1 / 2



Però com vaig comentar en diversos punts anteriors, la meva investigació es basa més a trobar el nou servei que ofereixen els grups criminals, el famós *"Ransomware as a Service"*. En aquesta investigació a la *Dark Web* he trobat dit servei i la cosa que més em va sorprendre és la disponibilitat del servei postvenda. A continuació podem veure captures d'aquest lloc web:

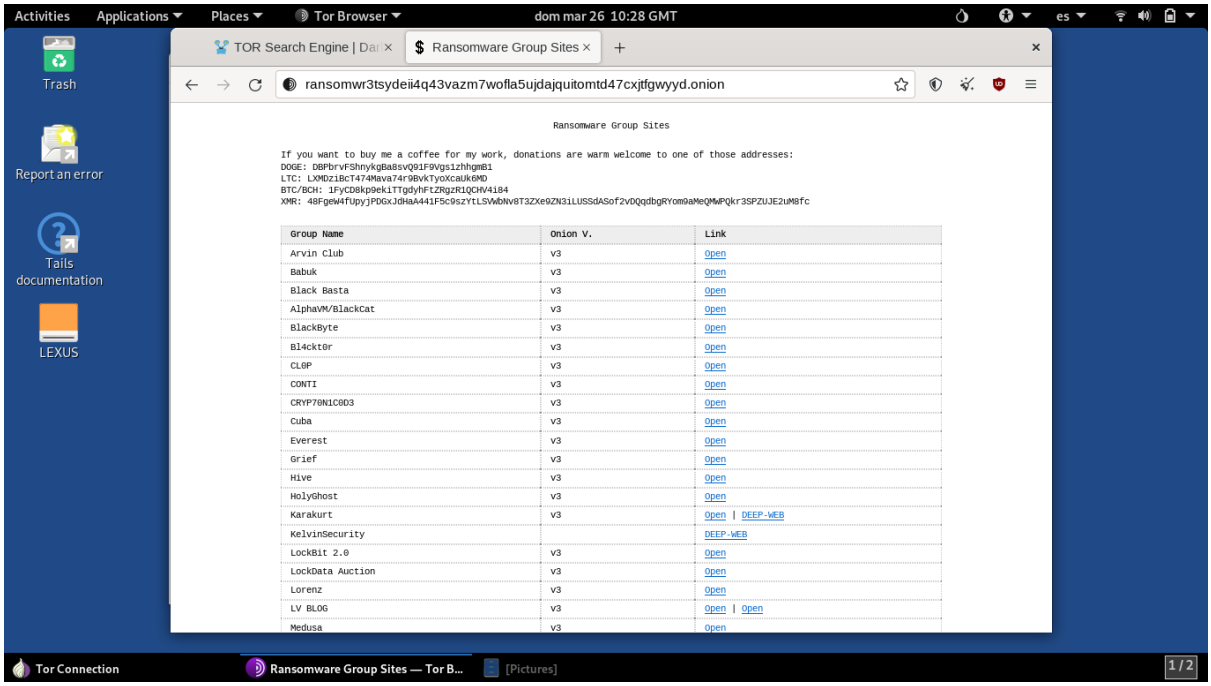




	Package #TEST	Package #STANDARD	Package #PREMIUM	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C2 Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Add-On: Dropper (+90 USD)	No	Buy	Yes	Yes
Add-On: Clone (+90 USD)	No	Buy	Buy	Yes
Add-On: FUD+ (+300 USD)	Buy	Buy	Buy	Yes
Add-On: Unkillable Process (+90 USD)	No	Buy	Buy	Yes
FUD Stub #	1	1 (100% private FUD stub)	2 (100% private FUD stub)	**6 (100% private FUD stub)**
Price	120 USD	490 USD	900 USD	1900 USD

Com podem veure avui dia, no fa falta ser un perfil molt tècnic per poder efectuar atacs a les empreses i poder lucrar-se dels rescats d'aquestes. Aspecte preocupant, ja que s'ha transformat literalment en un negoci d'empreses, il·legals, però és gent que té un producte i ho ven com si fos un "*Software as a Service*" (Netflix, Spotify, Google Docs, etc.).

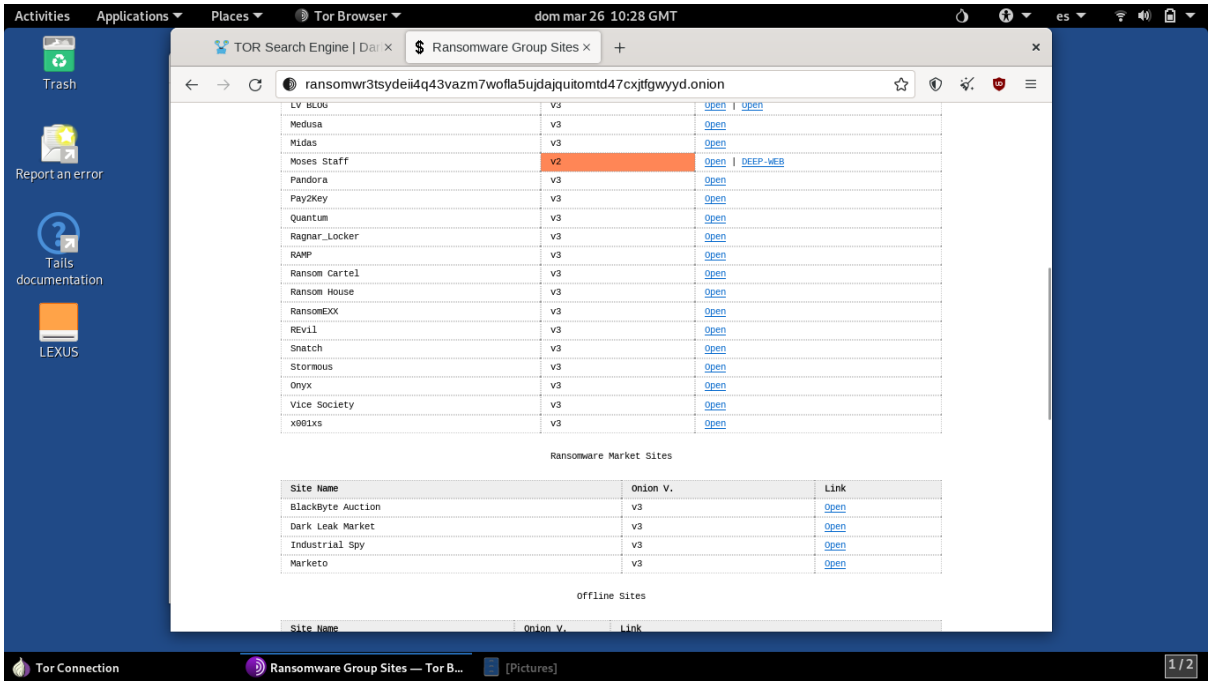
Podem veure que no és una cosa d'un cas específic i aïllat, ja que hi ha competència en aquest àmbit. En les imatges següents, trobem una pàgina que recopila la informació sobre les pàgines web dels grups de hackers i la disponibilitat de poder adquirir el seu *RaaS*.



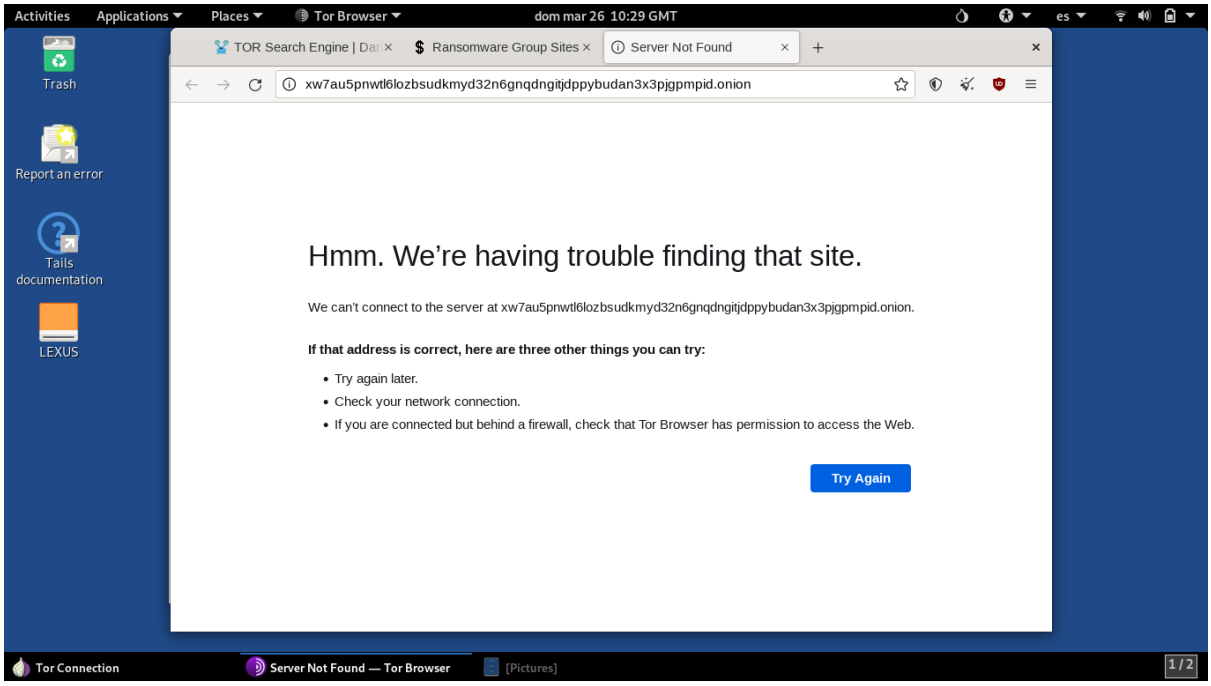
Ransomware Group Sites

If you want to buy me a coffee for my work, donations are warm welcome to one of those addresses:
DOGE: DBPbrvFShnykgBa8svQ91F9Vgs1zhhgmB1
LTC: LXMDziBcT474Mava74r9BvkTyoXcaUk6MD
BTC/BCH: 1FyCD8kp9ekiTTgdyhFtZRgzR1QCHV4184
XMR: 48FgeW4fUpyjPDGxJdHaA441F5c9szYtLSVWbNv8T3ZXe9ZN3iLUSSdASof2vDQqdbgRYom9aMeQMwPQkr3SPZUJE2uM8fc

Group Name	Onion V.	Link
Arvin Club	v3	Open
Babuk	v3	Open
Black Basta	v3	Open
AlphaVM/BlackCat	v3	Open
BlackByte	v3	Open
Bl4ckt0r	v3	Open
CL0P	v3	Open
CONTI	v3	Open
CRYPT0N1C0D3	v3	Open
Cuba	v3	Open
Everest	v3	Open
Grief	v3	Open
Hive	v3	Open
HolyGhost	v3	Open
Karakurt	v3	Open | DEEP-WEB
KelvinSecurity		DEEP-WEB
LockBit 2.0	v3	Open
LockData Auction	v3	Open
Lorenz	v3	Open
LV BLOG	v3	Open | Open
Medusa	v3	Open



Hi ha enllaços que ja no serveixen, perquè el grup de hackers ha sigut desmantellat com en el cas de "Hive"[36] o que volen desaparèixer com ara el grup de hackers "RansomHouse", responsables de l'atac a l'Hospital Clínic de Barcelona.


Activities
Applications
Places
Tor Browser
dom mar 26 10:29 GMT
es
Trash
Report an error
Tails documentation
LEXUS
TOR Search Engine | Dar
Ransomware Group Sites
Server Not Found
xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion
Hmm. We're having trouble finding that site.
We can't connect to the server at xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion.
If that address is correct, here are three other things you can try:
Try again later.
Check your network connection.
If you are connected but behind a firewall, check that Tor Browser has permission to access the Web.
Try Again
Tor Connection
Server Not Found — Tor Browser
[Pictures]
1 / 2

4. Asseguradores i els seus serveis contra els ciberatacs

En aquest punt del treball es farà una recerca sobre les ciberassegurances, és a dir, investigar quines cobertures poden tenir aquestes i veure si realment compleixen amb les necessitats que hi podrien tenir els clients. També durant aquest punt s'esmentaran les experiències des de dos punts de vista diferents, ja que s'han fet reunions amb la CEO d'una empresa d'assegurances, Maria Torra Badia (CEO de l'empresa Dracma) i amb el fundador d'una PIME, Felipe López Pinto (propietari de l'empresa Verbien).

4.1. Recerca sobre les asseguradores i les cobertures que ofereixen

S'ha elaborat una recerca sobre les cobertures que ofereixen les ciberassegurances i la majoria ofereix les mateixes cobertures i són les següents[37][38][39][40][41][42]:

- **Danys propis:**
  - Danys d'actius: L'empresa asseguradora es faria càrrec dels costos de reconstituir els actius digitals que es danyen, perden, alteren, corrompen o són robats. També dels danys físics dels equips TI.
  - Interrupcions del negoci: L'asseguradora es faria càrrec dels beneficis que no ha guanyat l'empresa, durant el ciberincident.
  - Pèrdues associades a la ciber extorsió: L'asseguradora es faria càrrec dels costos de la intervenció de consultors tecnològics, de RRPP, legals, negociadors i l'import exigit.
  - Reconstrucció d'imatge: L'asseguradora cobriria els costos dels serveis relacionats per a mitigar el mal produït a la reputació.
  - Despeses de gestió de crisis: Cobrir despeses d'assessorament al client, per a contenir, detenir, establir la causa i el seu abast, confirmant l'ocurrència de fets i identificant als afectats.
- **Danys a tercers:**
  - Responsabilitat Civil per violació de la privacitat.
  - Responsabilitat Civil d'activitat als mitjans de comunicació.

Dites cobertures depenen molt de l'empresa asseguradora, perquè cada condicionant està redactat de forma diferent i és difícil de generalitzar i comparar.

Totes o gairebé totes les empreses d'assegurances es basen en un qüestionari que fan al client, per saber quina quantia han de cobrar-li per donar-li cobertura o directament no acceptar-li la cobertura, les preguntes solen estar basades en els estàndards ISO 27000. Hi ha determinades activitat que directament no les cobreixen, perquè tenen moltes dades confidencials de clients, com podrien ser les assessores fiscals i laborals.

4.2. Entrevista amb la CEO d'una empresa d'assegurances

Es va celebrar el dia 27 de març una entrevista amb la Maria Torra Badia, CEO de l'empresa Dracma, una empresa d'assegurances i un dels serveis que ofereix dita empresa són les ciberassegurances. Aquesta entrevista es va fer amb l'objectiu de poder obtenir informació de primera mà d'una persona experta en el tema i veure des del seu punt de vista, el possible motiu del perquè els productes com les ciberassegurances no són tan populars.

Durant aquesta entrevista es van tractar sobretot els temes de la venda de les ciberassegurances a les empreses i les possibles dificultats que poden arribar a tenir per poder vendre productes d'aquest tipus. Finalment, es van arribar a unes conclusions molt interessants, les quals són molt útils per l'anàlisi final d'aquest treball.

Dites conclusions van ser les següents:

1. Les empreses no donen d'importància que se li ha de donar a la ciberseguretat, perquè no són molt coneixedores sobre el tema, com s'ha vist al punt 2.2 d'aquest treball, en el qual s'ha vist que encara hi ha un percentatge de PIMES (empreses que representen un nombre alt d'empreses a Espanya) que no saben de què tracta el terme ciberseguretat.

2. La part contrària al punt anterior és que hi ha empreses que creuen que porten molt bé la seguretat de la seva empresa, per aquest motiu no troben la necessitat de tenir aquesta despesa.

3. Hi ha empreses generalistes d'assegurances que volen oferir un servei nou, però sense desenvolupar el departament encarregat. Aquestes, després de veure que la freqüència i impactes dels ciberatacs tenen un creixement exponencial, com s'ha reflectit en el punt 2.1 i 2.2 del treball, ho han tancat momentàniament.

4. Relacionat amb la conclusió anterior i amb el punt 2.3 d'aquest treball, també surt reflectit la falta de talent en aquest àmbit, ja que ara està més de moda, tothom vol posicionar-se en el mercat i es vol fer ràpidament.

Amb les conclusions que se'n van arribar en aquesta entrevista, es contrastaran amb una opinió i experiència directa d'un propietari d'una empresa que ja va patir un ciberatac.

4.3. Entrevista amb el propietari d'una empresa que va patir un atac Ransomware

L'entrevista amb el propietari de l'empresa Óptica Verbien, Felipe López Pinto, es va celebrar el dia 26 de maig. Aquesta empresa es dedica a la venda d'ulleres graduades i audiòfons, la qual pot tenir dades confidencials dels seus clients. L'objectiu d'aquesta entrevista és per poder contrastar les conclusions del punt 4.2 d'aquest treball, ja que ara seria des del punt de vista del client.

L'any 2017 dita empresa va patir un ciberatac de tipus Ransomware, el qual va perjudicar l'activitat primària de l'empresa, perquè no tenien accés a cap mena de dades dels clients (punt molt important, perquè sense dades es feia difícil de treballar i estaven preocupats sobre l'exposició d'aquestes dades. Temes molt rellevants, els quals han estat tractats en el punt 1.2 del treball) i tampoc podien accedir al seu sistema d'informació per poder elaborar altres activitats, com la de registrar una compra d'un producte. Per aquest motiu en l'empresa son molt conscients sobre d'importància de la ciberseguretat i les repercussions que pot tenir un atac sobre el negoci y els seus stakeholders.
Durant aquesta entrevista hem tractat temes de seguretat a l'empresa, experiències que es va patir durant l'atac i l'opinió de les ciberassegurances.

Les conclusions van ser les següents:

1. Per molt que puguis tenir totes les proteccions necessàries per evitar patir un atac, sempre pots tenir una probabilitat, per baixa que pugui ser. També s'ha de tenir en compte molts punts del negoci (aquesta preocupació encara és creixent, perquè actualment han patit un hackeig a la targeta de crèdit de l'empresa), perquè es poden tenir incidències per molts punts.

2. Les empreses asseguradores han de fer més publicitat sobre els serveis dels seus productes referents a la ciberseguretat. Es va arribar a aquesta conclusió durant l'entrevista, perquè Felipe més d'un dia es volia informar sobre nous productes referents a la ciberseguretat a les empreses, però les asseguradores (s'ha de clarificar que eren asseguradores molt conegudes, però no es mencionaran) no acabaven de tenir els coneixements necessaris per poder vendre satisfactòriament el producte. Amb l'experiència esmentada es podria relacionar amb la conclusió número 3 de l'entrevista del punt 4.2, ja que fa menció sobre la poca preparació del personal de les asseguradores.

3. Sobre la mateixa experiència d'intentar informar-se sobre productes de ciberseguretat a les asseguradores, el propietari de l'empresa es va trobar que molts dels productes tenien cobertures que ja té d'uns altres, fent-li la sensació que li farien pagar diversos cops el mateix. A tot això s'ha de mencionar de quan es preguntava si era el mateix, el servei de vendes de les assegurances no sabia bé les diferències de les cobertures.

5. Conclusions sobre com es podria millorar la venda de les ciber assegurances

Abans de començar amb les conclusions s'ha de matisar que només s'ha fet l'entrevista a una empresa d'assegurances (la qual és bastant experta en les ciberassegurances) i a una PIME (la qual està en una bona posició quant a ciberseguretat), és a dir, que l'anàlisi podria haver sigut major, però és bastant complicat aconseguir una entrevista amb empreses per parlar-ne de ciberseguretat. També les conclusions de com es podrien incrementar les vendes aniria dirigit més al nínxol de les PIMES, pel fet que formen part d'un percentatge molt elevat a Espanya (les grans empreses només formen part del 0,17% segons què s'ha vist al punt 2.2).

Primerament, es podria detectar que hi ha molt desconeixement de la ciberseguretat a les PIMES, perquè només el 68% sap que engloba el termini de ciberseguretat o saben de la seva existència. Així mateix, un 64% de les PIMES porta la ciberseguretat internament, un 20% s'encarrega un familiar o amic i un 12% ningú s'encarrega. Només el 38% de les empreses tenen externalitzat aquest servei a una empresa especialitzada (Verbien forma part d'aquest percentatge). A part de les dades tractades al punt 2.2 del treball, a la conclusió número 1 de l'entrevista a la CEO de Dracma, també es fa referència al fet que les empreses no li donen importància a la ciberseguretat.

La bretxa de professionals és bastant gran i cada cop és major (com s'ha vist al punt 2.3), ja que és del 26% segons el report de Deloitte i un percentatge del 57% a Catalunya. Això ocasiona un problema bastant gran, perquè per aquest mateix motiu les empreses no poden tenir el personal que realment necessiten, en aquest cas les asseguradores per poder ser capaces de vendre aquest tipus de producte o a les mateixes PIME per poder protegir-se més. També aquest punt es veu reflectit a la pràctica en ambdues entrevistes, tant per la part de les assegurances (Dracma), com la del client (Verbien).

També relacionat amb el desconeixement de la ciberseguretat, les empreses no veuen la necessitat de tenir una ciberassegurança, perquè no són coneixedors de les repercussions que poden tenir, tant d'imatge, com legals. Tothom sap que ha de tenir una assegurança amb una cobertura d'incendis, perquè sap molt bé les repercussions que pot tenir. A aquest punt és on s'hauria d'arribar, de trobar-ho com una solució en el cas es pateixi un ciberatac.

Després d'arribar a aquestes conclusions, es pot veure que es podrien fer diverses coses per poder millorar la venda de les ciberassegurances per part de les mateixes empreses asseguradores. Unes propostes podrien ser les següents:

1. Les empreses d'assegurances haurien de fer més divulgacions referents a la ciberseguretat, ja que jugaria a favor seu la conscienciació de les persones que porten les empreses. Es podria fer el símil amb el patrocini d'influenciadors o microinfluenciadors, perquè a la gent en informar-la d'una cosa al final li crea la necessitat de tenir-ho.

2. També les empreses asseguradores podrien impartir formacions als seus treballadors sobre ciberseguretat, tant com per poder vendre els productes de la mateixa empresa i alhora serviria per conscienciar a les persones que treballen a la mateixa organització.

3. Referent al producte, es podria millorar, ja que com comenta Felipe (propietari de Verbien) sembla que hi ha cobertures que ja cobreixen altres productes. Es podrien fer més personalitzats segons les necessitats del client, sobretot si ja és client de la mateixa asseguradora. També es podria anant actualitzant segons les noves necessitats de seguretat, perquè és un món que no para de créixer i els ciberdelinqüents sempre busquen noves maneres d'actuar i evidentment fer-ho saber al client, perquè ho tingui en compte com a factor diferenciador, sobretot de les ciberassegurances de la competència.

Amb aquestes possibles millores per poder vendre més les ciberassegurances, s'intentaria transformar a un perfil que no sap sobre ciberseguretat, a un perfil més coneixedor del tema (el qual implica que tindrà més preocupacions i les haurà de solucionar). També que els possibles clients que es preocupen per a la seva ciberseguretat, puguin ser coneixedors dels productes i poder optar a un producte de qualitat. En últim lloc, la part de la formació del personal de les asseguradores, forma una part molt important de la venda, perquè un bon producte difícilment es pot vendre sol i es necessitaria millorar els seus coneixements per poder assessorar amb una qualitat superior.

6. Bibliografia

[1] *¿Qué es la seguridad de datos? Definición y descripción general de la seguridad de datos | IBM*. (s.d.). Recuperat 24 febrer 2023, de https://www.ibm.com/es-es/topics/data-security

[2] *¿Qué es seguridad de la información (InfoSec)? | Seguridad de Microsoft*. (s.d.). Recuperat 24 febrer 2023, de https://www.microsoft.com/es-ww/security/business/security-101/what-is-information-security-infosec

[3] *¿Qué es el Big Data? Importancia y Aplicaciones | UNIR Colombia*. (s.d.). Universidad Virtual. | UNIR Colombia - Maestrías y Grados virtuales. Recuperat 24 febrer 2023, de https://colombia.unir.net/actualidad-unir/que-es-big-data/

[4] *Cómo afectan los ciberataques a su negocio | LinkedIn*. (s.d.). Recuperat 24 febrer 2023, de https://www.linkedin.com/pulse/c%C3%B3mo-afectan-los-ciberataques-su-negocio-fernando-pe%C3%B1a-merino/?originalSubdomain=es

[5] Marte, C. (s.d.). *Todo lo que debes saber sobre la NORMA ISO 20000*. Recuperat 24 febrer 2023, de https://www.ambit-bst.com/blog/todo-lo-que-debes-saber-sobre-la-norma-iso-20000

[6] Congreso de los Diputados - Canal Parlamento (Director). (2018, novembre 8). *Comisión Mixta de Seguridad Nacional (08/11/2018)*. https://www.youtube.com/watch?v=5SQ6ntnkYdo

[7] Yahoo reconoce que sufrió un «hackeo» que afectó a 1.000 millones de cuentas de usuario. (s.d.). *BBC News Mundo*. Recuperat 24 febrer 2023, de https://www.bbc.com/mundo/noticias-38324372

[8] *115 cybersecurity statistics + trends to know in 2023*. (s.d.). Recuperat 24 febrer 2023, de https://us.norton.com/blog/emerging-threats/cybersecurity-statistics

[9] McLennan, M., & Group, S. (s.d.). *The Global Risks Report 2021 16th Edition*.

[10] McLennan, M., & Group, S. (s.d.). *The Global Risks Report 2015 10th Edition*.

[11] *How Many Cyber Attacks Happen Per Day in 2023?* (s.d.). Techjury. Recuperat 24 febrer 2023, de https://techjury.net/blog/how-many-cyber-attacks-per-day/

[12] Thomas, I. (2022, desembre 16). *The FBI is worried about a wave of cyber crime against America's small businesses*. CNBC. https://www.cnbc.com/2022/12/16/fbi-7-billion-lost-in-criminal-hacks-most-victims-small-businesses.html

[13] *MAP | Kaspersky Cyberthreat real-time map*. (s.d.). MAP | Kaspersky Cyberthreat Real-Time Map. Recuperat 24 febrer 2023, de https://cybermap.kaspersky.com

[14] Gonzalo, M. (2022, març 1). *Guerra híbrida: Estos son los ciberataques que ha sufrido Ucrania*. Newtral. https://www.newtral.es/rusia-ucrania-cronologia-de-una-ciberguerra-ciberataques/20220301/

[15] *Stuxnet: ¿Qué es y cómo funciona?* (s.d.). Stuxnet: ¿Qué es y cómo funciona? Recuperat 24 febrer 2023, de https://www.avast.com/es-es/c-stuxnet

[16] *GreyNoise*. (s.d.). Recuperat 24 febrer 2023, de https://www.greynoise.io

[17] Caño, A. (2013, febrer 19). Estados Unidos y China, ante la primera ciberguerra fría. *El País*. https://elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html

[18] Aguiar, A. R. (2021, març 21). *EEUU, Rusia y China protagonizan una ciberguerra que se ha convertido en el juego de espías más sofisticado de la historia: Estas son las armas con las que cuenta cada uno*. Business Insider España. https://www.businessinsider.es/guerra-fria-disputan-hackers-eeuu-china-rusia-829767

[19] Cárdenas, M. J. (2022, desembre 27). Ciberespionaje desde China. *LISA News*. https://www.lisanews.org/ciberseguridad/ciberespionaje-desde-china/

[20] Perlroth, N. (2021, juliol 19). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

[21] *¿Qué es una botnet?* (s.d.). ¿Qué es una botnet? Recuperat 24 febrer 2023, de https://www.avast.com/es-es/c-botnet

[22] 'Informe_Cibercriminalidad_2021_.pdf'. Available: https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf

[23] 'Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf'. Available: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

[24] *Cifras PYME. Datos enero 2022*. (2022).

[25] 'deloitte-es-risk-advisory-estado-de-la-ciberseguridad-en-espana-2022.pdf'. Available: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/riesgos/deloitte-es-risk-advisory-estado-de-la-ciberseguridad-en-espana-2022.pdf

[26] *Number of ransomware attacks per year 2022*. (s.d.). Statista. Recuperat 24 febrer 2023, de https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

[27] Cable, J. (s.d.). *Ransomwhere*. Recuperat 24 febrer 2023, de https://ransomwhe.re/

[28] Aguiar, A. R. (2023, gener 22). *El pago de rescates por «ransomware» se desploma en 2022 más de un 40%: Las víctimas ya no quieren pagar más a los ciberdelincuentes*. Business Insider España. https://www.businessinsider.es/pago-rescates-ransomware-desplome-2022-40-por-ciento-1187756

[29] *Ciberseguretat a Catalunya 2023*. (s.d.). Recuperat 25 febrer 2023, de https://www.accio.gencat.cat/web/.content/bancconeixement/documents/pindoles/ACCIO-ciberseguretat-a-catalunya-pindola-tecnologica-ca.pdf

[30] *The Tor Project | Privacy & Freedom Online*. (s.d.). Recuperat 25 març 2023, de https://torproject.org

[31] *¿Qué es una VPN y cómo funciona?* (s.d.). ¿Qué es una VPN y cómo funciona? Recuperat 25 març 2023, de https://www.avast.com/es-es/c-what-is-a-vpn

[32] *Tails*. (s.d.). Recuperat 25 març 2023, de https://tails.boum.org/

[33] Daniels, N. (2020, maig 1). *Cómo Acceder de Forma Segura a la Dark Web en 15 Pasos*. VPNOverview.com. https://vpnoverview.com/es/privacidad/navegacion-anonima/acceder-a-la-dark-web/

[34] *Virtualization Technology & Virtual Machine Software: What is Virtualization?* (s.d.). VMware. Recuperat 25 març 2023, de https://www.vmware.com/solutions/virtualization.html

[35] *Tails—Install Tails from Windows*. (s.d.). Recuperat 26 març 2023, de https://tails.boum.org/install/windows/index.en.html

[36] *Desmantelada una infraestructura del grupo criminal HIVE dirigida a realizar ataques de ransomware por todo el mundo*. (s.d.). Recuperat 2 abril 2023, de http://platon:10100/opencms/ca/detalle/articulo/Desmantelada-una-infraestructura-del-grupo-criminal-HIVE-dirigida-a-realizar-ataques-de-ransomware-por-todo-el-mundo/

[37] *Seguro Ciberriesgos Pyme y Autónomos—Seguros MAPFRE. (s.d.). MAPFRE ESPAÑA. Recuperat 20 maig 2023, de* https://www.mapfre.es/empresas/seguro-ciberriesgos/

[38] *Ciber seguros para empresas | Hiscox. (s.d.). Recuperat 20 maig 2023, de* https://www.hiscox.es/seguros/ciberseguridad

[39] *Coberturas de un Seguro de Riesgos Cibernéticos – Globalfinanz Seguro responsabilidad administradores*. (s.d.). Recuperat 20 maig 2023, de https://www.responsabilidadconsejerosydirectivos.com/coberturas-seguro-riesgos-ciberneticos/

[40] *Markel, & España, M. (2022, abril 8). ¿Qué es un Ciberseguro? Coberturas y Precios | Markel España. Markel.* https://markel.com.es/blog/responsabilidad-civil/ciberseguro/

[41] Broking, E. R. &. (2023, març 30). *Seguros de Ciberriesgo: Guía sobre sus coberturas | WTW*. WTW Update. https://willistowerswatsonupdate.es/ciberseguridad/guia-sobre-la-cobertura-de-los-ciberriesgos/

[42] *Seguros de empresa*. (s.d.). DRACMA. Recuperat 20 maig 2023, de https://dracma.cat/esp/empresas/seguros-de-empresa