Basque CyberSecurity Centre

Zibersegurtasunaren egoera Euskadin

2022ko 4. hiruhilekoa

Basque CyberSecurity Centre

Erantzukizunetik salbuesteko klausula

Dokumentu hau BCSC-k erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko ematen da. BCSC ezin izango da, inola ere, zuzenean edo zeharka, jakinarazitako informazioa eta BCSC-ren webguneko zein kanpoko informazioko teknologiak ustekabean edo ezohiko moduan erabiltzeak eragin ditzakeen kalteen erantzuletzat jo, baldin eta kanpoko web-orrialdeetara, sare sozialetara, software-produktuetara edo alertan edo BCSC-ren webgunean ager daitekeen beste edozein informaziora estekatuta sartzen bada. Nolanahi ere, alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako terminoen araberako iritziak eta gomendioak dira, eta ezin da ondorio juridiko loteslerik sortu jakinarazitako informaziotik.

Saltzeko debekuaren klausula

Erabat debekatuta dago edozein onura ekonomiko saltzea edo lortzea, hargatik eragotzi gabe dokumentu hau kopiatu, banatu, hedatu edo zabaltzeko aukera.

Basque CyberSecurity Centre

Edukia

1. Laburpen exekutiboa 4
2. Gertaera garrantzitsuak 5
    2.1. Nazioarteko eremua 5
    2.2. Estatuko eremua 7
    2.3. Euskadiko eremua 8
3. BCSCk kudeatutako gertaerak 8
4. Zaurgarritasunak 9
5. Malwarea 16
    5.1. Erabilitako teknikak 19
    5.2. Ransomwarea 21
6. Phishinga 24
7. Gomendio orokorrak 25
8. Bibliografia 27

Basque CyberSecurity Centre

1. Laburpen-txostena

Txosten hau Zibersegurtasuneko Euskal Zentroak etengabe gainbegiratu eta ebaluatu du, Euskadin eragina izan dezaketen mehatxuak identifikatzeko, neurri egokiak ezartze aldera. Txostenean, 2022ko azken hiruhilekoan izandako gertaera eta mehatxu esanguratsuenak bildu eta aztertu dira. EAEko erakunde publikoen, enpresen eta herritarren zibermehatxuen aurrean prebentzio-, detekzio- eta erantzun-gaitasunak hobetzeko informazio erabilgarria biltzen du txostenak.

Euskadiko zibersegurtasunaren egungo egoera ulertzeko, funtsezkoa da nazioarteko errealitatearen ikuspegi globala izatea ekosistema digitala baldintzatzen duten hainbat alderditan.

Errusia eta Ukrainaren arteko gatazka, neurri handi batean, nazioarteko egoeraren faktore erabakigarria izaten jarraitzen du, 2022. urte osoan gertatu den bezala. Errusiaren eta Ukrainaren arteko zibererasoak % 50 murriztu dira, eta Ukrainaren aurkako 70 zibereraso eta Errusiar Federazioaren aurkako 25 zibereraso jakinarazi dira. Hala ere, gatazkan dauden herrialdeen mugetatik kanpo, eraso horiek bikoiztu egin dira aurreko aldiarekin alderatuta, eta guztira 239 izan dira. Erasorik ohikoena banatutako zerbitzua ukatzea (DDoS) da. Informazio-ihesak, malwareak eta phishingak ere jakinarazi dira. Ildo horretan, Errusiarekin lotura handiena duten jardule maltzurrak Sandworm eta Gamaredon izan dira, besteak beste. Aliatu berriak nabarmentzen dira, hala nola AITahrea irakiarra. Ukrainaren aldetik, IT Army of Ukraine da aliaturik aktiboena.

Bestalde, araudiaren ikuspegitik, Europako Parlamentuak NIS2 zuzentarauaren eta DORA erregelamenduaren aplikazioa onartu du. Horiek zibersegurtasunerako eta erresilientzia digitalerako esparru berria formalizatzen dute finantza-zerbitzuetan eta, oro har, Europar Batasunean. Arauketa berriak aurreko legeak bateratu nahi ditu, baina, aldi berean, betebehar berriak dakartza, industria mota desberdinek legeak betetzen dituztela bermatzeko.

Estatuan, hainbat albiste garrantzitsu izan dira, hala nola Bartzelonako 3 ospitaleri eragin zien zibereraso bat, Telefonicak jasotako zibereraso bat eta Polizia Nazionalak phishingean aritzen zen erakunde kriminal bat desegin izana.

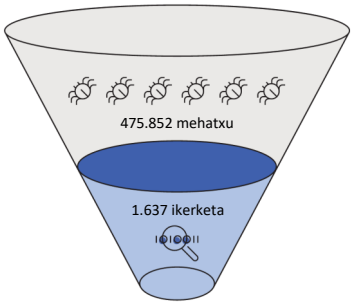
2022ko laugarren hiruhilekoan, Euskadin nabarmentzekoa da Noticias Taldeak jasotako zibererasoa (inprimatutako edizioei eragin zien), bai eta finantza-erakundeetako bezeroei SMS faltsuen bidez iruzur egiten zien Arabako banda bat desegin izana ere. Gainera, Zibersegurtasuneko Euskal Zentroak 208 gertakari kudeatu ditu, eta horien tipologia ohikoena iruzurra da.

Detektatutako zaurgarritasunei dagokienez, aldi horretan 6.751 argitaratu dira. Horrek esan nahi du % 2,03ko jaitsiera izan dela aurreko hiruhilekoaren aldean, orduan 6.888 erregistratu baitziren. Halaber, zaurgarritasun kritikoak % 13,71 murriztu dira, aldi honetan 1.014 erregistratu baitira, aurreko hiruhilekoan 1.153 erregistratu ondoren. Gainerako zaurgarritasunei dagokienez, CVSSaren V3 balorazioaren arabera, 2.435k balorazio altua dute, 2.613 ertainak dira, 123 baxuak dira eta 566 esleitzeko daude informazioa aukeratzeko unean. Zaurgarritasunaren tipologia ohikoena cross-site-scripting (XSS) da. Bestalde, zaurgarritasunen aldetik kalte handiena jasan duten produktuak Googlerenak (Android-ekin lotutakoak), Microsoftenak edo Mozillarenak izan dira.

Era berean, aldi horretan 31 zaurgarritasun berri identifikatu dira, eta erasotzaileek aktiboki ustiatzen dituzte.

Laugarren hiruhilekoan, 4.129 malware-infekzio identifikatu dira. Malware-tipologia gisa, ransomwareak mehatxu garrantzitsua izaten jarraitzen du. Hiruhileko honetan, 390 malware-infekzio identifikatu dira. Ildo horretan, talde kriminal aktiboenak Lockbit, Bian Lian eta BlackCat izan dira.

2022ko laugarren hiruhilekoan, 475.852 mehatxu-zantzu identifikatu dira, eta, hasierako prozesatze eta iragazte baten ondoren, 1.637 ikerketa eragin dituzte, bakoitzari dagokion analisiarekin. Ildo horretan, informazio-ihesak eragin handiena duen mehatxuetako bat izaten jarraitzen du, nahiz eta aztertutako aldiaren amaieran kredentzialen lapurretak gorakada izan duen.



ITURRIA: BCSC-REN ADIMEN-EREDUA

2. Gertaera garrantzitsuak

Mundu hiperkonektatu batean bizi gara, beharrezkoa baita enpresek beren negozioak garatzeko, bai eta gizartea garatzeko ere, oro har, maila pertsonalean zein profesionalean, esparru guztietan. Testuinguru horren barruan, erakundeen ziberdefentsa-gaitasunak eraiki behar dira, ez bakarrik tokian tokiko ikuspegitik begiratuta, baizik eta nazioarteko errealitatea ere kontuan hartuta. Horretarako, hainbat alderditan (soziala, ekonomikoa, politikoa, etab.) gizartearen errealitatea etengabe aldatzen duten joerak aztertu behar dira, baita "ziber" munduan dituzten ondorioak ere, dauden arriskuak arintzeko eta egokitzeko modu egokian erreakzionatu ahal izateko, erresilientzian lagunduz eta, zalantzarik gabe, lehiakortasunean lagunduz.

Hori dela eta, urteko laugarren hiruhilekoko ekitaldi garrantzitsuenak laburbiltzen dira txosten honetan, Euskadin nazioarteko, estatuko eta tokiko mailan gertatutakoak. Horrela, erakundeei azterketa zehatz hori eginez, etorkizuneko arriskuak prebenitzeko eta, oro har, haien defentsa-gaitasunak hobetzeko funtsezkotzat jotzen dugun informazioa eskaintzen diegu.

2.1. Nazioarte maila

2022ko laugarren hiruhilekoan nabarmenak dira Errusiaren eta Ukrainaren arteko gatazkatik eratorritako ziberespazioko jarduerak

Nazioarteko egoeraren analisiari dagokionez, 2022ko laugarren hiruhilekoan nabarmenak dira Errusiaren eta Ukrainaren arteko gatazkatik eratorritako ziberespazioko jarduerak.

Egoera nazioartean aztertuz gero, laugarren hiruhilekoan, 2022an gertatu den bezala, Errusia eta Ukrainaren arteko gatazkak eragindako ondorioak izan dira nagusi. Errusiak Kharkiv eta Kherson eskualdeetan atzera egin ondoren gatazka itxuraz gelditu den arren, ziberespazioko gudu-zelaian Errusiar Federazioan jakinarazitako zibererasoen kopurua ia erdia izan da, aurreko aldiarekin alderatuz gero. Hala ere, berriz ere herrialde gerrazaleen mugetatik kanpo egindako zibererasoen kopurua bikoiztu egin da, eta gehienak NATOko herrialdeen mugen barruan daude.

Eragina jasan duten sektore nagusiak hauek izan dira: sektore publikoa, finantzarioa, energetikoa, administratiboa eta garraiokoa, eta, ondoren, IKT sektorea, fabrikazioa eta komunikabideak. Ukrainak jasandako zibererasoei dagokienez, badirudi finantza-zerbitzuak, energia-sektoreko ordainketa-sistemak, komunikabideak eta logistikoak erabilezin bihurtzera eta administrazio publikoak blokeatzera bideratu direla. Ekintza horiek koherenteak dirudite Errusiako armadak Ukrainako azpiegitura kritikoaren aurkako gudu fisikoan misil eta drone suiziden bidez egindako erasoekin, gatazkak aurrera egin ahala gertaeren bilakaeraren errepresalian. Bestalde, helburu errusiarren aurkako zibererasoak antzekoak izan dira, baina ez dira hainbeste izan.

Laugarren hiruhilekoan, 70 zibereraso jasan zituen Ukrainak, 25 Errusiako Federazioak eta 239 zibereraso munduko gainerako herrialdeetan.

2022ko azken lauhilekoan munduko gainerako herrialdeetan erregistratutako 239 erasoetatik, 213 NATOko herrialdeei zuzendu zaizkie, batez ere gatazkaren inguruan dauden eta Ukrainari estaldura ematen dioten herrialdeei, hala nola Poloniari (70), Letoniari (33), Lituaniari (16) eta Estoniari (11). Bestalde, 22 zibereraso erregistratu dira Estatu Batuetan eta 12 Erresuma Batuan, horiek ere gatazkarekin lotuta. Azkenik, azpimarratzekoak dira Txekiar Errepublikan erregistratutako 15 zibererasoak. Herrialdeko hainbat sektore estrategikori eragin zieten, eta aldi berean gertatu ziren urriaren 3an eta azaroaren 11n.

NATOn ez dauden eta zibereraso gehien jasan dituzten herrialdeen artean, Moldavia nabarmentzen da, 11 zibereraso erregistratu baititu, gatazka armatuaren ondorioek ondoko herrialdean jasandako krisi larriagotuaren ondorioz bere gobernuaren politiken aurkako protesta masiboek tenkatutako barne egoera batekin batera.

Era berean, zibererasoen tipologiari dagokionez, laugarren hiruhilekoan hirugarren hiruhilekoan atzemandako joerak jarraitu du. Izan ere, erregistratutako ia zibereraso guztiak banatutako zerbitzua ukatzeagatiko (DDoS) erasoak dira, eta, aurreko aldiarekin alderatuta, 100 eraso berri baino gehiago izan dira. Beste alde batetik, Informazio Ihesa (Hack & Leak), Malware edo Phishingagatik gertatutakoak ere jakinarazi dira, neurri txikiagoan. Laugarren lauhilekoan erregistratutako joera sendotzeak berekin dakar ziberespazioaren esparruan gatazkan inplikatutako eragileen defentsa-gaitasunak hobetzea, Malware, Wiper, Ransomware edo sarrerako bektore nagusia diren Phishing-erasoen aurrean, DDoS erasoetara bideratuz erasotzeko gaitasun ia guztiak.

DDoS erasoetan sakonduz gero, guztira 310 zibereraso erregistratu dira, eta horietatik 61 Ukrainako helburuen aurka gertatu dira. Soilik 13k izan dute Errusiar Federazioa helburu, eta 236 mundu osoan erregistratu dira; horietatik gehienak, lehen esan bezala, NATOko herrialdeetan gertatu ziren. Eragindako sektoreak oso heterogeneoak izan dira, baina batez ere administrazio publikoak, energia- eta finantza-sektorea, bai eta garraioarena, IKTena, komunikabideena eta industriarena ere.

Azkenik, Errusiari zuzenean lotutako jardule maltzur aktiboenak Sandworm eta Gamaredon izan dira, People 's Cyber Army, Phoenix, Anonymous Russia, XakNet, Killnet, Clowns, Russian Hackers Team, FRwL eta NoName057 (16) eta antzeko kolektiboekin batera. Horiek oso aktiboki hartu dute parte lauhileko osoan. Errusiaren aliatu berrien artean, nabarmentzekoa da AlTahrea jardule irakiarrak urriaren 8an Ukrainako tren-azpiegituraren aurka egindako erasoa. Bestalde, Ukrainarekin lotura zuzena duen jardule nagusia, IT Army of Ukraine, berriz ere aktiboena izan da laugarren lauhilekoan, kausa ukrainarraren alde dauden eragile guztien artean. Hala ere, Moskuko erregimenaren aurkako kolektiboek egindako hainbat eraso nabarmentzen dira. Kolektibo horiek, besteak beste, hauek dira: National Republican Army kolektiboa, Putinek Errusiaren barruan bultzatutako politiken aurkariek osatua, edo Cyber Partisans, Bielorrusiako kolektibo bat, helburu errusiarren aurkako zibererasoak ere egin dituena. Errusiaren eta Ukrainaren arteko gatazkaz gain, nazioarteko beste gertakari interesgarri batzuk ere jazo dira.

- **Pirata informatikoek defentsarako base industrialeko erakunde bati nola eraso zioten jakinarazi dute FBIk, CISAk eta NSAk**[I]. Ameriketako Estatu Batuetako zibersegurtasun- eta inteligentzia-agentziek urriaren 4an jakitera eman zutenez, litekeena da pirata informatiko nazionalen talde batzuek defentsa-base industrialaren sektoreko erakunde baten enpresa-sareari eraso izana ziberespioitza kanpaina baten parte gisa. Aurkikuntzak CISAk Mandiant zibersegurtasuneko enpresarekin elkarlanean 2021eko azarotik 2022ko urtarrilera bitartean izandako gertakariei erantzuteko ahaleginen emaitza dira. Bidegabe sartzea ez zaio egotzi jardule edo mehatxu-talde ezagun bati.
- **Zibereraso batek Bulgariako Gobernuaren webguneak eten ditu "Errusiari traizio egiteagatik".**[II] Banatutako zerbitzua ukatzeko (DDoS) eraso batek presidentearen administrazioaren, Defentsa Ministerioaren, Barne Ministerioaren, Justizia Ministerioaren eta Konstituzio Auzitegiaren webguneak erorarazi zituen denbora labur batez. Dnevnik online argitalpen bulgariarraren arabera, sarbidea berrezarri ondoren, guneek ohi baino motelago funtzionatzen zuten. Killnet pirata informatiko errusiazaleen taldeak erasoaren egiletza aldarrikatu zuen, "Errusiari traizioa egiteagatik eta Ukrainari armak emateagatik" zigorra zela esanez.
- **Europako Parlamentuaren webgunea hackeatu dute Errusiarekin ebazpen kritiko bat onartu ondoren.**[III] Europako Parlamentuaren webguneak banatutako zerbitzua ukatzeko (DDoS) eraso zibernetiko bat jasan zuen, eta horrek orrialdera sartzea galarazi zion gutxienez ordubetez. Euroganberako taldeak lanean

ari dira egoera konpontzeko. Killnet talde errusiazaleak bere gain hartu du erasoa Telegrameko kanalean. Talde hori bera Etxe Zuriko, errege-etxe britainiarreko eta Frantziako zenbait administraziotako zerbitzu informatikoen aurkako beste eraso batzuen atzean dagoela susmatzen da. Hala ere, Parlamentuko iturriek ezin izan dute erasotzaileen nortasuna egiaztatu.

- **Hackerrek ransomware bidez eraso dio defentsa australiarreko komunikazio-plataforma bati.**[IV] Mehatxu-agenteek ransomware-erasoa egin dute Australiako militarrek eta defentsakoek erabilitako komunikazio-plataforma baten aurka. ForceNet izeneko enpresa Defentsa Sailaren kanpo-zerbitzuen hornitzaileetako bat da, bere webguneetako bat kudeatzeko kontratatuta baitago.
- **Indiako pirata informatikoek Pakistango politikarien eta jeneralen ordenagailuei eraso diete.**[V] Badirudi helburu politikoetako batzuk India eta Pakistanen arteko etengabeko tentsioetatik sortuak direla. Urtarrilaren 10ean, taldeak Fawad Chaudhryren helbide elektronikoan sartzeko agindua jaso zuen. Orduan, Fawad Chaudhry Imran Khan lehen ministroaren gobernuko Informazio ministroa zen. Fawad Chaudhryren sarrerako ontziaren pantaila-irudi bat atera zuten, eta Sunday Times-ek eta Bureau-k ikusi zuten.
- **Urriaren amaieran, zibereraso batek trenak geldiarazi zituen Danimarkan. Erasoak kanpoko informatika-zerbitzuen hornitzaile bati eragin zion.**[VI] Zibereraso baten ondorioz, Danimarkako DBS enpresak trenen prestakuntza gelditu behar izan zuen joan den asteburuan, eta mehatxuaren eragileek hirugarrenen TI zerbitzuen hornitzaile bat eraso zuten. Erasoak Danimarkako Supeo enpresari eragin zion, enpresa-aktiboak kudeatzeko irtenbideak ematen baitizkie tren-konpainiei, garraio-azpiegituren operadoreei eta bidaiarien agintari publikoei. DSB Danimarkako tren-enpresarik handiena da.

2.2. Estatu maila

Laugarren hiruhilekoan, Estatu mailan albiste ugari eman dira zibersegurtasunari buruz eta jardule maltzurren azterketari buruz. Hona hemen gertakari garrantzitsu horien laburpena:

- **Zibereraso batek Bartzelonako hiru ospitaleri kalte egin die.**[VII] Bartzelonako zenbait ospitalek zibereraso bat jasan zuten, eta sistema informatikoak erabili ezinik geratu ziren. Hiru ospitalek eta hainbat anbulatoriok eta egoitzek kalteak izan zituzten, eta gorabeherak izan zituzten espezialisten kontsultetan beharrezkoak ziren hainbat gailuren erabileran.
- **Telefonicak zibererasoa jasan zuen urrian.**[VIII] Telefonicak bezeroei jakinarazi zien, zibereraso baten ondorioz, wifi-routerren pasahitzak aldatu behar zituztela, bai etxeetan, bai enpresetan. Bizitegi- eta enpresa-routerren sarbide-gakoak arriskuan jarri ziren. Hala ere, zibererasoak ez du berekin ekarri datu pertsonalak lapurtzea, hala nola izena, helbidea, NANa, deien historia edo bankuko datuak.
- **Polizia Nazionalak phishinga egiten zuen erakunde kriminala desegin du.**[IX] Polizia Nazionalak "CEOren iruzurra" erabiliz iruzurrak egiten espezializatutako erakunde kriminal bat desegin du, eta 15 kide atxilotu ditu: bederatzi Madrilen, bost Albaceten eta beste bat Valentzian. Poliziaren ikerketari esker, sare hori iruzurrezko transferentzia askorekin (850.000 euroko balioarekin, gutxi gorabehera) lotu da, baita jasotzen zuten dirua jaso eta zuritzen zuen enpresa-sare batekin ere.

2.3. Euskadi maila

2022ko laugarren hiruhilekoan, zibersegurtasuneko gertakari hauek nabarmendu dira Euskadiko ingurune geografikoan:

- **Noticias Taldearen aurkako zibererasoa.**[X] Egindako eraso zibernetiko batek arazoak sortu zituen Noticias Taldea egunkariko orri inprimatuen ekoizpenean. Ondorioz, egunkariaren zerbitzariak blokeatu egin ziren eta Noticias Taldea osatzen duten inprimatutako lau edizioei eragin zieten: Arabakoari (Noticias de Álava), Nafarroakoari (Noticias de Navarra), Gipuzkoakoari (Noticias de Gipuzkoa) eta Bizkaikoari (DEIA). Horrek zalantzan jarri zuen egunkariaren edizio inprimatuak garaiz eskuratu ahal izatea kioskoetan, nahiz eta Noticias de Álavak bertan egotea eta unean uneko informazioa eskaintzea lortu zuen.
- **SMS faltsuekin finantza erakundeetako bezeroei iruzur egiten zien talde bat desegin dute Araban.**[XI] Polizia Nazionalak finantza-erakundeetako bezeroei iruzur egiten zien talde bat desegin du Araban, testu-mezu faltsuen bidez. Ikerketen arabera, Basauriko espetxean espetxeratuta zeuden bi pertsonak zuzentzen zuten talde kriminala, eta, ustez, handik ematen zizkieten argibideak taldeko gainerako kideei. Polizia Nazionalaren Polizia Judizialeko Brigada Probintzialak gidatu zuen operazioa, Gasteizen, eta aukera eman zuen herrialde osoan internet bidez iruzurrak egiten zituen taldearen jarduerei amaiera emateko.

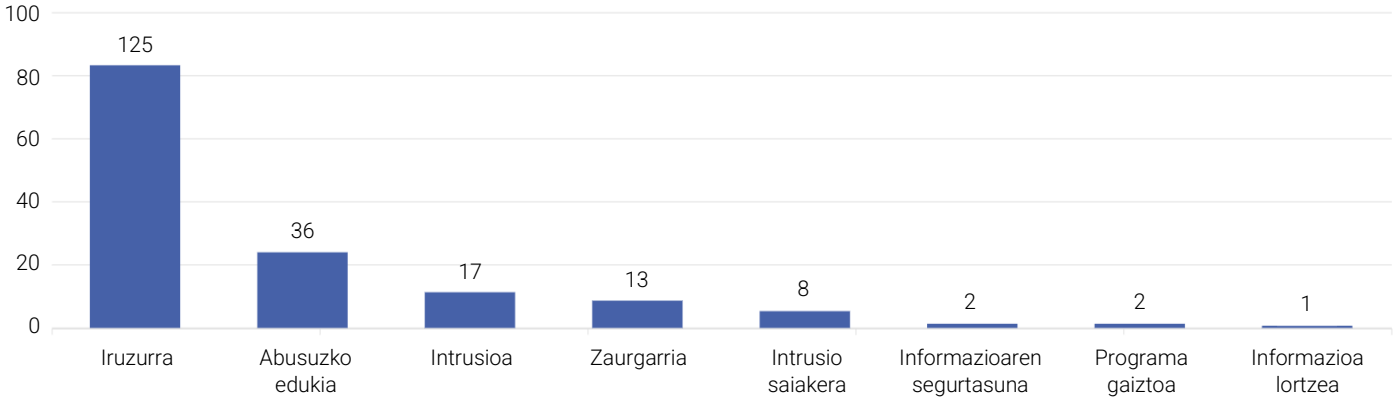
3. BCSCk kudeatutako gertaerak

2022ko laugarren hiruhilekoan 208 gertakari kudeatu dira, eta tipologia ohikoena iruzurra izan da.

2022ko laugarren hiruhilekoan 208 gertakari kudeatu dira, eta tipologia ohikoena iruzurra izan da.

Gertakari horiek herritarrak, enpresak eta erakunde publikoak dira, eta informazioa ematen diote Zibersegurtasuneko Euskal Zentroko aholkularitza-zerbitzuari. Edozein jarduera susmagarri identifikatuz gero, eskertuko genizuke incidencias@bcsc.eus helbide elektronikoaren bidez edo **900 104 891** telefonora deituz jakinaraztea, mehatxua arintzeko neurri tekniko egokiak hartu ahal izateko.

BCSCk kudeatutako gertaeren tipologiak



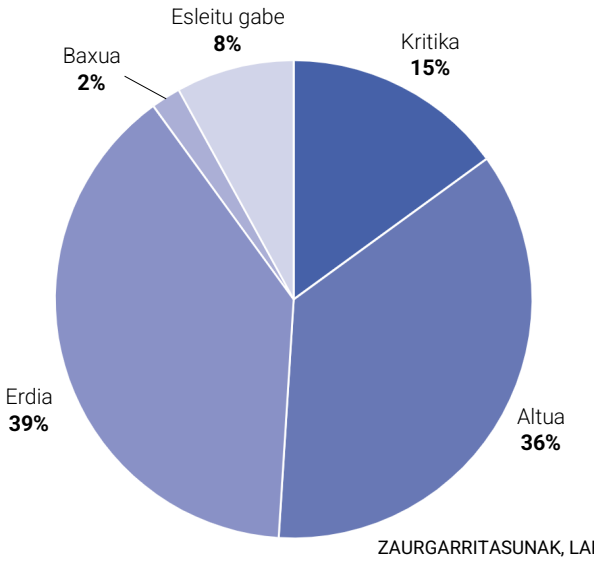
BCSCK KUDEATUTAKO GERTAEREN TIPOLOGIAK. ITURRIA: BCSC

4. Zaurgarritasunak

Aldi horretan 6.751 zaurgarritasun berri argitaratu dira, hau da, aurreko hiruhilekoan baino % 2,03 gehiago.

Aldi horretan 6.751 zaurgarritasun berri argitaratu dira, hau da, aurreko hiruhilekoan baino % 2,03 gehiago, orduan 6.888 izan baitziren. Halaber, zaurgarritasun kritikoak % 13,71 murriztu dira, eta aldi horretan 1.014 erregistratu dira, aurreko hiruhilekoan 1.153 izan ondoren. Gainerako zaurgarritasunei dagokienez, CVSSaren V3 balorazioaren arabera, 2.435k balorazio altua dute, 2.613 ertainak dira, 123 baxuak dira, eta 566 esleitzeko daude informazioa aukeratzeko unean.

Zaurgarritasunak, larritasunaren arabera

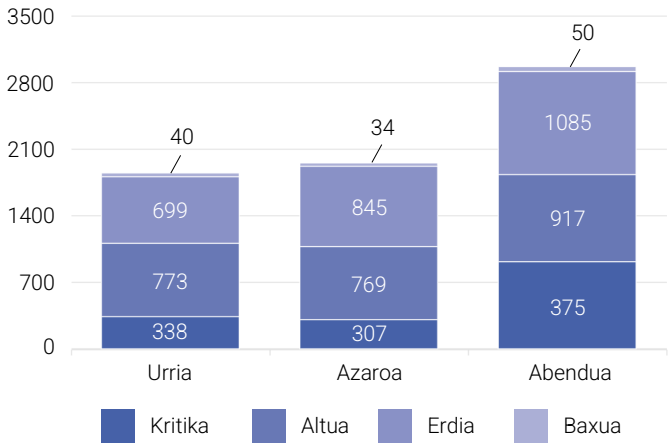


ZAURGARRITASUNAK, LARRITASUNAREN ARABERA. ITURRIA: MITRE

Zaurgarritasun bakoitza desberdina da eta modu desberdinean eragiten die aktiboei. Batzuek urruneko kodea exekutatzea ahalbidetzen dute, beste batzuek kodea edo jarraibideak injektatzea eta programa baten portaeran eragina izatea, beste batzuek pribilegioak eskalatzea ahalbidetzen dute, etab.

Kritikotasun horrek eta zaurgarritasun kopuru osoak bilakaera izan dute hiruhileko honetan, jarraian adierazten den moduan:

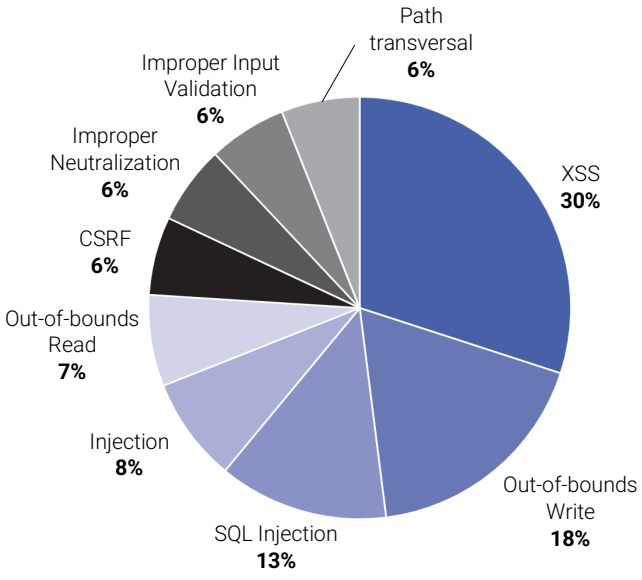
Kritikotasunaren bilakaera, hilabeteka



ZAURGARRITASUNEN BILAKAERA, LARRITASUNAREN ARABERA. ITURRIA: MITRE

CWE (Common Weakness Enumeration) estandarra oinarritzat hartuta eta zaurgarritasun mota aztertuta, honela banatzen dira:

Zaurgarritasun-moten TOP 10a

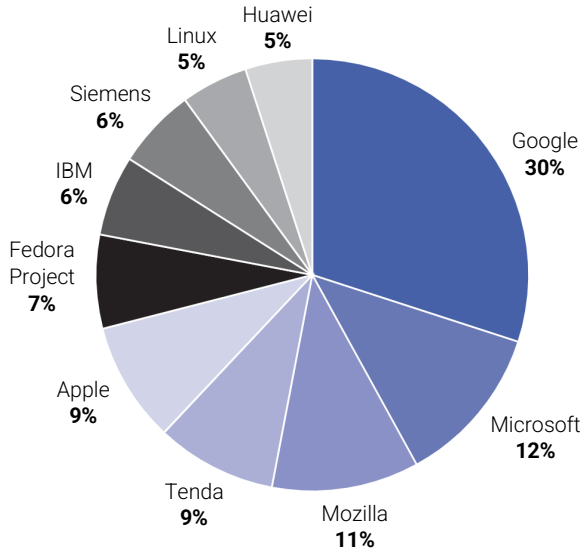


ZAURGARRITASUN-MOTEN TOP 10A. ITURRIA: MITRE

Ikus daitekeenez, aztertzen ari garen hiruhilekoan, cross-site-scripting (XSS) zaurgarritasun motak ohikoena izaten jarraitzen du.

Eragindako fabrikatzaileei dagokienez, hurrengo grafikoan ikus daiteke hiruhileko honetan argitaratutako zaurgarritasunen eraginpean daudenen TOP 10ari:

Zaurgarritasunak, fabrikatzailearen

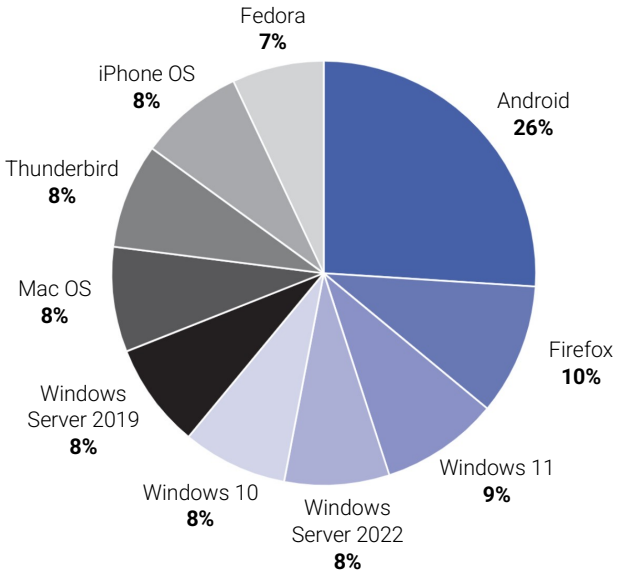


ZAURGARRITASUNEN ERAGINPEKO FABRIKATZAILEEN TOP 10A. TURRIA: MITRE

Ikus daitekeenez, gehien erabiltzen diren produktuetako batzuen fabrikatzaileak Google (Android bezalako produktuen bidez), Microsoft edo Mozilla dira.

Eragindako produktuaren araberako zaurgarritasunen zerrenda grafiko honetan ikus daiteke:

Ahuleziak produktuaren arabera



ZAURGARRITASUNEK ERAGINDAKO PRODUKTUEN TOP 10A. ITURRIA: MITRE

Ikus daitekeenez, lotura mantentzen da fabrikatzaileen aurreko grafikoarekin.

Era berean, aldi honetan 31 zaurgarritasun berri identifikatu dira, eta erasotzaileek aktiboki ustiatzen dituzte.

Hiruhileko honetan identifikatutako zaurgarritasun guztietatik, eta hainbat irizpide kontuan hartuta, hala nola larritasuna bera, ustiapen aktiboa eta inpaktu potentziala, honako hauek nabarmentzen dira:

CVE-2022-4116

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-4116
- CWE: 94
- Eragindako produktuak: Quarkus
- CVSS balorazioa: 9.8 KRITIKOA CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: Altua
- Osotasuna: Altua
- Erabilgarritasuna: Altua

Zaurgarritasun bat aurkitu da Quarkusen. Segurtasun-akats hau Dev UI Config Editore-n gertatzen da. Kaltebera da drive-by localhost erasoen aurrean, eta kodeak urrunetik exekutatzea dakar.

CVE-2022-42856

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-42856
- CWE: 843
- Eragindako produktuak: Safari, tvOS, macOS Ventura, iOS, iPadOS
- CVSS balorazioa: 8.8 ALTUA CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Beharrezkoa
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

Motak nahasteko arazo bat konpondu da, egoeren kudeaketa hobetuta. Arazoa bertsio hauetan zuzendu da: 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 eta iPadOS 15.7.2, iOS 16.1.2 Web-edukia modu maltzurrean diseinatuta prozesatzeak kode arbitrarioa betearaztea ekar dezake. Applek badaki arazo hau aktiboki ustiatu ahal izan dela iOS 15.1 baino lehen jaurtitako iOS bertsioen aurka.

CVE-2022-31705

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-31705 https://www.ciberseguridad.eus/ultima-hora/vulnerabilidades-en-productos-vmware
- CWE: 787
- Eragindako produktuak: VMware vRealize Network Insight (vRNI), VMware ESXi, VMware Workstation y VMware Fusion.
- CVSS balorazioa: 8.2 ALTUA CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
- Eraso-bektorea: Lokala
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Altuak
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketekin
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

VMware ESXi, Workstation eta Fusion sistemek mugetatik kanpo idazteko zaurgarritasuna dute USB 2.0 kontrolagailuan (EHCI). Makina birtual batean pribilegio administratibo lokalak dituen jardule maltzur batek arazo hau ustiatu dezake hostean exekutatzen den makina birtualaren VMX prozesua bezalako kodea exekutatzeko. ESXi-n, ustiapena VMX sandboxaren barruan dago, eta Workstation eta Fusion-en, berriz, horrek kodea exekutatzea ekar dezake Workstation edo Fusion instalatuta dagoen makinan.

CVE-2022-44710

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-44710 https://www.ciberseguridad.eus/ultima-hora/actualizaciones-de-seguridad-de-microsoft-de-diciembre-de-2022
- CWE: 269
- Eragindako produktuak: DirectX Graphics Kernel
- CVSS balorazioa: 7.8 ALTUA CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
- Eraso-bektorea: Lokala
- Konplexutasuna: Altua
- Eskatutako pribilegioak: Baxua
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketekin
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

Pribilegioak jasotzeko zaurgarritasuna DirectX grafikoen nukleoan.

CVE-2022-20419

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-20419 https://www.ciberseguridad.eus/ultima-hora/boletin-de-seguridad-de-android-de-octubre-de-2022
- CWE: Informazio eskasa
- Eragindako produktuak: Android
- CVSS balorazioa: 7.8 ALTUA CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Lokala
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Baxua
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

ActivityRecord.java-ren setOptions-en, abiarazte-prozesuan edozein Java kode arbitrario kargatzeko aukera dago, kodean akats logiko bat dagoelako. Horrek pribilegio lokalen eskalada ekar lezake, exekuzio-pribilegio gehigarrien beharrik gabe. Ez da behar erabiltzailearen interakziorik ustiapenerako.

Jarraian, industria-inguruneei eta produktuei dagokienez, zaurgarritasun garrantzitsuenak adierazten dira.

CVE-2022-3156

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-3156 https://www.ciberseguridad.eus/ultima-hora/control-de-acceso-inadecuado-en-rockwell-automation-studio-5000-logix-emulate
- CWE: 287
- Eragindako produktuak: Rockwell Automation Studio 5000 Logix Emulate softwarea
- CVSS balorazioa: 7.8 ALTUA CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: tokikoa
- Konplexutasuna: Baxuak
- Eskatutako pribilegioak: Baxuak
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

Kodea urrunetik exekutazeko zaurgarritasuna du Rockwell Automation Studio 5000 Logix Emulate softwareak. Softwarea instalatzen denean, erabiltzaileei baimen handiak ematen zaizkie produktuaren zerbitzu jakin batzuetan. Konfigurazio oker horren ondorioz, asmo txarreko erabiltzaile batek kodea urrunetik exekutatu lezake xede-softwarean.

CVE-2022-43509

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-43509 https://www.ciberseguridad.eus/ultima-hora/escritura-fuera-de-limites-en-omron-cx-programmer
- CWE: 787
- Eragindako produktuak: CX-Programmer v.9.77 eta aurrekoa
- CVSS balorazioa: 7.8 ALTUA CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- Eraso-bektorea: tokikoa
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Beharrezkoa
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

CX-Programmer v.9.77 bertsioaren eta aurrekoen mugetatik kanpo idazteko zaurgarritasuna dago, eta horrek informazioa zabaltzea eta/edo kode arbitrarioa betearaztea ekar dezake, erabiltzaile batek CXP fitxategi bat bereziki diseinatuta irekiz.

CVE-2022-3087

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-3087 https://www.ciberseguridad.eus/ultima-hora/ejecucion-de-codigo-arbitrario-en-productos-de-fuji-electric
- CWE: 787
- Eragindako produktuak: Fuji Electric Tellus Lite V-Simulator 4.0.12.0 bertsioa eta aurrekoak.
- CVSS balorazioa: 7.8 ALTUA CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
- Eraso-bektorea: tokikoa
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Beharrezkoa
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: Altua
- Osotasuna: Altua
- Erabilgarritasuna: Altua

Fuji Electric Tellus Lite V-Simulator 4.0.12.0 bertsioak eta aurrekoak mugetatik kanpo idazteko zaurgarritasuna dute, eta, hala, erasotzaile batek kode arbitrarioa exekuta dezake.

CVE-2022-40263

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-40263 https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-de-credenciales-sin-cifrar-en-bd-totalys-multiprocessor
- CWE: 798
- Eragindako produktuak: BD Totalys MultiProcessor 1.70 bertsioa eta aurrekoak.
- CVSS balorazioa: 7.8 ALTUA CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: tokikoa
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Baxua
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: Altua
- Osotasuna: Altua
- Erabilgarritasuna: Altua

BD Totalys MultiProcessor 1.70 bertsioak eta aurrekoek kredentzial kodetuak dituzte. Baliatuz gero, mehatxuek informazio konfidentziala eskuratu, aldatu edo ezabatu dezakete, babestutako osasun-informazio elektronikoa (ePHI), babestutako osasun-informazioa (PHI) eta identifikazio pertsonaleko informazioa (PII) barne. Microsoft Windows 10ekin BD Totalys MultiProcessor 1.70 bertsioa erabiltzen duten bezeroek sistema eragilea gogortzeko konfigurazio gehigarriak dituzte, eta zaurgarritasun hori ustiatzeko behar den erasoaren konplexutasuna handitzen dute.

CVE-2022-33324

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-33324 https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-dos-en-productos-mitsubishi-electric
- CWE: 404
- Eragindako produktuak: Mitsubishi Electric Corporation MELSEC iQ-R Series R00/01/02CPU
- CVSS balorazioa: 7.5 ALTUA CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: Bat ere ez
- Osotasuna: Bat ere ez
- Erabilgarritasuna: Altua

Kautotu gabeko urruneko erasotzaile bati aukera ematen dio moduluaren Ethernet komunikazioan zerbitzua ukatzeko, horretarako diseinatutako paketeak bidaliz. Berreskurapenerako moduluaren sistema berrabiarazi behar da.

Era berean, zibersegurtasun-esparruko produktu batzuek zaurgarritasunak dituzte. Garrantzitsua da horien berri izatea; izan ere, gure sistemen segurtasuna produktu horiengan delegatzen badugu, zaurgarritasun batek erasotzaile baten aurrean jar ditzake. Jarraian, hiruhileko honetan argitaratu diren segurtasun-produktuen eta teknologien zaurgarritasun garrantzitsuenak erakusten dira:

CVE-2022-27518

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-27518 https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-critica-en-citrix-adc-y-citrix-gateway
- CWE: 664
- Eragindako produktuak: Citrix ADC, Citrix Gateway
- CVSS balorazioa: 9.8 KRITIKOA CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

Kode arbitrarioaren urrutiko exekuzioa kautotu gabe.

CVE-2022-42475

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-42475 https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-critica-en-fortios
- CWE: 787
- Eragindako produktuak: FortiOS SSL-VPN, FortiProxy SSL-VPN
- CVSS balorazioa: 9.8 KRITIKOA CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

FortiOS SSL-VPN 7.2.0tik 7.2.2ra, 7.0.0tik 7.0.8ra, 6.4.0tik 6.4.10era, 6.2.0tik 6.2.11ra, 6.0.15era eta aurrekoetan eta FortiProxy SSL-VPN 7.2.0tik 7.2.1, 7.0.7ra eta aurrekoetan heap [CWE-122]-an oinarritutako buferrak gainezka egiteko zaurgarritasun batek aukera eman diezaioke kautotu gabeko urruneko erasotzaile bati kodea edo komando arbitrarioak exekutatzeko, berariaz diseinatutako eskaeren bidez.

CVE-2022-33873

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-33873 https://www.ciberseguridad.eus/ultima-hora/inyeccion-de-comando-no-autenticado-en-fortitester
- CWE: 78
- Eragindako produktuak: FortiTester, bertsioak: 7.1.0 eta 7.0.0; 4.2.0, 4.1.0tik 4.1.1era eta 4.0.0; 3.9.0tik 3.9.1era, 3.8.0, 3.7.0tik 3.7.1era, 3.6.0, 3.5.0tik 3.5.1era, 3.4.0, 3.3.0tik 3.3.1era, 3.2.0, 3.1.0 eta 3.0.0; 2.9.0, 2.8.0, 2.7.0, 2.6.0, 2.5.0, 2.4.0tik 2.4.1era eta 2.3.0.
- CVSS balorazioa: 9.8 KRITIKOA CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

OS ('OS Command Injection') komando batean erabilitako elementu berezien neutralizazio oker batek [CWE-78] zaurgarritasunak eragiten ditu hauetan: FortiTester 2.3.0tik 3.9.1era, 4.0.0tik 4.2.0ra, 7.0.0tik 7.1.0ra, eta komando arbitrario bat exekutatzeko aukera eman diezaiokete kautotu gabeko erasotzaile bati azpiko shellean.

CVE-2022-40684

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-40684 https://www.ciberseguridad.eus/ultima-hora/aviso-de-seguridad-fortios-y-fortiproxy
- CWE: 306
- Eragindako produktuak: FortiOS: 7.0.0tik 7.0.6ra eta 7.2.0tik 7.2.1era, FortiProxy: 7.0.0tik 7.0.6ra eta 7.2.0
- CVSS balorazioa: 9.8 KRITIKOA CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Baxua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

CVE-2022-0030

- Erreferentzia: https://nvd.nist.gov/vuln/detail/CVE-2022-0030 https://www.ciberseguridad.eus/ultima-hora/vulnerabilidad-en-pan-os-de-palo-alto-cve-2022-0030
- CWE: 290
- Eragindako produktuak: Palo Alto Networks PAN-OS 8.1
- CVSS balorazioa: 8.1 ALTUA CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- Eraso-bektorea: Sarea
- Konplexutasuna: Altua
- Eskatutako pribilegioak: Bat ere ez
- Erabiltzailearen elkarrekintza: Bat ere ez
- Irismena: Aldaketarik gabe
- Konfidentzialtasuna: **Altua**
- Osotasuna: **Altua**
- Erabilgarritasuna: **Altua**

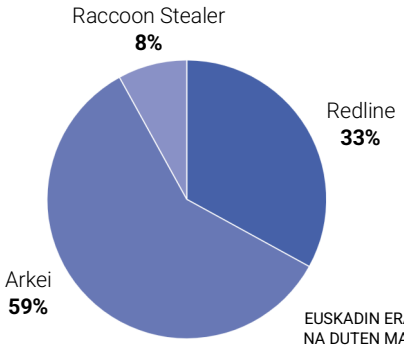
Palo Alto Networks-en PAN-OS 8.1 web interfazean autentifikaziorik ez izatearen zaurgarritasun batek aukera ematen dio suebakiaren edo helmugako panoramaren ezagutza espezifikoak dituen sarean oinarritutako erasotzaile bati PANen administratzaile baten plantak egiteko eta ekintza pribilegiatuak egiteko.

5. Malwarea

2022ko laugarren hiruhilekoan malware-familia desberdinen 356 infekzio identifikatu dira.

BCSCk Euskadin eragin-tasa handiena duten malware-familiak monitorizatzen ditu. 2022ko laugarren hiruhilekoan malware-familia desberdinen 300 infekzio baino gehiago identifikatu dira. Honela banatu dira:

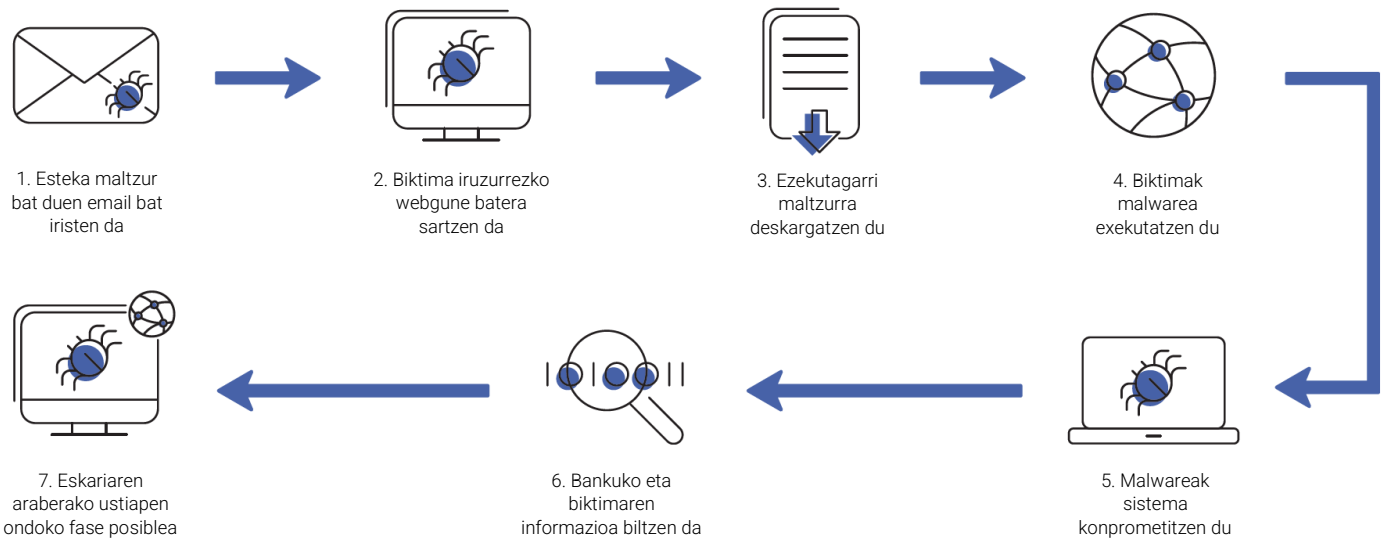
Euskadin eragin handiena duten malwareak



EUSKADIN ERAGIN HANDIENA DUTEN MALWARE FAMILIEN TOP 5A. ITURRIA: BCSC

REDLINE

Redline Stealer (RedLine izenez ere ezaguna) software maltzurra da, 150 eta 200 dolar artean eros daitekeena, bertsioaren arabera, hackerren foroetan. Redline datuak lapurtu eta sistema eragileak malwarearekin infektatu ditzake. Oro har, ziberdelitugileak ordenagailuak RedLine Stealer bezalako software maltzurrarekin infektatzen saiatzen dira, lapurtutako informazioa behar ez bezala erabiliz dirua sortzeko eta sistemak helburu berarekin mota horretako software gehigarriarekin infektatzeko. Honako elementu hauei buruzko datuak biltzeko gai da: ekipoa eta sistema eragilea, fitxategiak, nabigatzaileak, VPN bezeroak, ftp bezeroak, mezularitza-bezeroak, jokoen bezeroak eta kriptomoneten zorroak.



REDLINEREN ERASO-KATEA. ITURRIA: BCSC

Aztertutako laginen eta ikusitako eraso tipikoen arabera, malware horren infekzioan erabilitako teknikak honako hauek dira:

Initial Access	Execution	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Phishing	User Execution	Credentials from Password Stores	Account Discovery	Data from local system	Non-Standard Port	Exfiltration Over C2 Channel
Spearphishing Attachment		Credentials from Web Browsers	Process Discovery	Screen Capture		
Spearphishing Link		Password Managers	Software Discovery			
Spearphishing via Service		Window Credential Manager	Security Software Discovery			
		OS Credential Dumping	System Time Discovery			
		Steal Web Session Cookie				
		Unsecured Credentials				
		Credentials In Files				
		Credentials In Registry				
		Group Policy Preferences				
		Private Keys				

REDLINE MALWAREAREN TTPAK. ITURRIA: BCSC

ARKEI

Arkei malware bat da, 2018ko maiatzetik ezaguna, informazio-lapurretan espezializatua. Erasotzaileak definitutako patroi batekin bat datozen nabigatzaileen, kriptomoneten eta fitxategien datuak biltzen ditu (erasotzaile bakoitzak bere patroiak zehaztu ditzake).

Pertsonalizatzeko gaitasuna dutenez, aldaera berriak ateratzen dira etengabe, eta zaila da eraso-mekanismo zehatz bat identifikatzea.

Honako hauek dira malwarearen TTPak komunak:

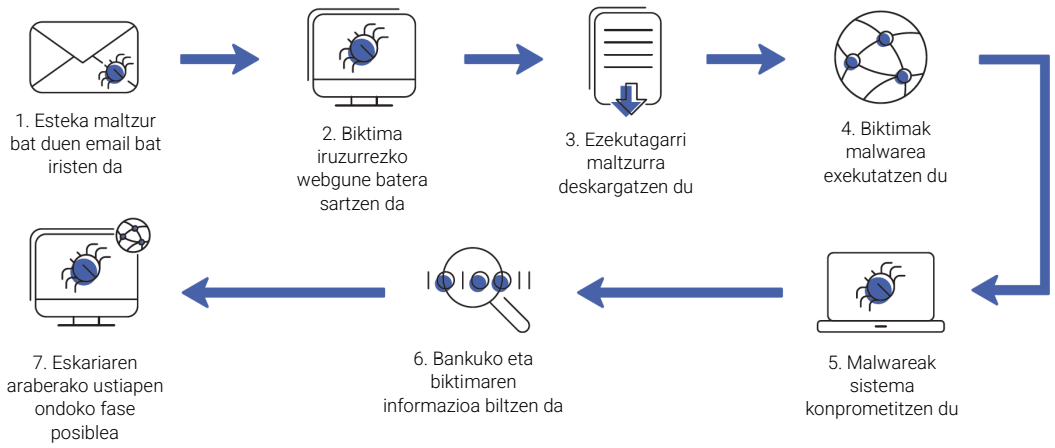
Execution	Credential Access	Discovery
Command and Scripting Interpreter	OS Credential Dumping	Query Registry

ARKEI MALWAREAREN TTPS. ITURRIA: BCSC

RACCOON STEALER:

Raccoon Stealer informazio-lapur ugarienetako bat izan zen 2021ean, eta hainbat eragile ziberkriminalek erabili zuten. Lehen, malware gisa saltzen zen foro klandestinoetako zerbitzu gisa 2019ko hasieratik, baina haren funtzionamendua bat-batean gelditu zen 2022ko martxoaren 25ean. 2022ko ekainaren 10ean, Shodan bilatzailean lapurrak administratzeko panelak bilatzen ari zirela, SEKOIA.IOko analistek "Raccoon Stealer 2.0" izeneko web-orria ostatatzen zuten zerbitzari aktiboekin topo egin zuten.

Software honen gaitasunak biktimei buruzko informazioa eskuratzean oinarritzen dira, eta honako hauek lortzeko gai dira: nabigatzailearen historia, kriptomoneten zorroak, posta elektronikoko helbideak, pasahitzak, cookieak, pantaila-kapturak, sistemaren informazioa. Hori da infekzio-fluxua.



RACCOON STEALEREN ERASO-KATEA. ITURRIA: BCSC

Malware honek erabiltzen dituen TTPak irudi honetan ageri dira:

Initial Access	Execution	Defense Evation	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Drive-by Compromise	Command and Scripting Interpreter	Deobfuscate/ Decode Files or Information	Credentials from Password Stores	Account Discovery	Archive Collected Data	Application Layer Protocol	Exfiltration Over C2 Channel
Phishing	Exploitation for Client Execution	Obfuscated Files or Information	Credentials from Web Browsers	File and Directory Discovery	Automated Collection	Data Encoding	
	Native API		Input Capture	Process Discovery	Data from Local System	Non-Application Layer Protocol	
			OS Credential Dumping	Query Registry	Email Collection		
			Unsecured Credentials	Remote System Discovery	Input Capture		
			Credentials in Files	System Information Discovery	Screen Capture		
				System Network Configuration Discovery			
				System Owner/ User Discovery			
				System Time Discovery			

RACCOON STEALER-EN TTP-AK. ITURRIA: BCSC.

5.1. Erabilitako teknikak

Malware-familiak erabilitako TOP 5 teknikak oinarri hartuta, horiek guztiak alderatu dira, gehien zein errepikatzen diren identifikatzeko, eta emaitza honako hau izan da:

Hurrengo grafikoan, Mitre Att&ck matrizearen arabera, azken hiruhilekoan Euskadin eragin handiena izan duten malwarean kokatutako ohiko TTPak zehazten dira. Teknika bakoitza 1 (berdea) eta 4 (gorria) arteko balio batekin puntuatzen da. Puntuazio altuagoak esan nahi du teknika malware-familia gehiagok erabiltzen duela.

EUSKADIN ERAGIN HANDIENA DUTEN MALWAREETAN OHIKOAK DIREN TTPAK.
ITURRIA: BCSC

Jarraian, gehien erabiltzen den teknika bakoitzaren deskribapen zehatza adierazten da; deskribapen hori, gutxienez, aztertutako malware-familien erdietan ikusitako tekniketarako egingo da:

Execution

- T1059 - Command and Scripting Interpreter: Aurkariek komando eta scripten interpreteak gehiegi erabil ditzakete komandoak, scriptak edo artxibo bitarrak exekutatzeko. Interfaze eta lengoaia horiek sistemen elkarreragiteko moduak eskaintzen dituzte, eta ezaugarri komuna dira plataforma desberdin askotan. Sistema gehienek komando-lerroko interfaze integratua eta komando-sekuentzien gaitasunak dituzte; adibidez, macOS eta Linux banaketek Unix Shell motaren bat dute, eta Windowsen instalazioek, berriz, Windows Command Shell eta PowerShell. Erasotzaileek hainbat modutan erabil ditzakete teknologia horiek, komando arbitrarioak gauzatzeko bitarteko gisa. Komando eta script-ak biktimentzako hasierako sarbide gisa erabil daitezke, dokumentu erakargarriak bidalita edo lehendik dagoen C2 batera bigarren mailako dei gisa. Aurkariek ere komandoak exekutatu ditzakete terminal/shell interaktiboen bidez, eta urruneko hainbat zerbitzu erabil ditzakete urrunetik exekutatzea lortzeko.

Credential access

- T1555.003 – Credentials from Web Browsers: Erasotzaileek web-nabigatzaileen kredentzialak eskura ditzakete, helburuko nabigatzailearen berariazko fitxategiak irakurriz. Web nabigatzaileek kredentzialak gorde ohi dituzte, hala nola erabiltzaile-izenak eta webguneen pasahitzak, etorkizunean eskuz sartu beharrik ez izateko. Web-nabigatzaileek kredentzialak formatu zifratu batean gorde ohi dituzte kredentzialen biltegi baten barruan; hala ere, web nabigatzaileetatik testu lauan kredentzialak ateratzeko metodoak daude.
- T1003 – OS Credential Dumping: Aurkariek sistema eragilearen kredentzialak iraultzen saia daitezke kontuaren saio-hasiera eta kredentzialaren edukia lortzeko, sistema eragilearen eta softwarearen hash edo testu-pasahitz argi moduan normalean. Gero, kredentzialak alboko mugimenduak egiteko eta informazio mugatua eskuratzeko erabil daitezke.
- T1552-001 – Unsecured Credentials: Credentials In Files: Aurkariek artxibo lokalen sistemak eta urruneko artxiboen baliabide partekatuak bila ditzakete, segurtasunik gabe gordetako egiaztagiriak dituzten artxiboen bila. Hauek izan daitezke erabiltzaileek beren kredentzialak gordetzeko sortutako fitxategiak, pertsona-talde batentzat partekatutako kredentzialen biltegiak, sistema edo zerbitzu baterako pasahitzak dituzten konfigurazio-fitxategiak, edo pasahitz txertatuak dituzten iturri-kodeko fitxategi bitarrak.

Discovery

- T1087 – Account Discovery: Erasotzaileek kontuen zerrenda bat lortzen saia daitezke sistema batean edo ingurune baten barruan. Informazio hori lagungarri izan dakieke aurkariei jarraipen-portaeran laguntzeko zer kontu dauden zehazteko.
- T1012 – Query Registry: Erasotzaileek Windowseko erregistroarekin elkarreragin dezakete instalatutako sistemari, konfigurazioari eta softwareari buruzko informazioa biltzeko. Erregistroak informazio ugari biltzen du sistema eragileari, konfigurazioari, softwareari eta segurtasunari buruz.
- T1057 – Process Discovery: Erasotzaileak sistema batean gauzatzen ari diren prozesuei buruzko informazioa lortzen saia daitezke. Lortutako informazioa sareko sistemetan exekutatzen diren softwarea eta aplikazio komunak ezagutzeko erabil liteke. Erasotzaileek prozesuen aurkikuntzari buruzko informazioa erabil dezakete aurkikuntza automatizatuan, ondorengo portaerei forma emateko, kontuan hartuta aurkariak helburua erabat infektatzen duen edota ekintza espezifikoak egiten saiatzen ari den.
- T1124 – System Time Discovery: Erasotzaileek sistema lokal edo urruneko baten ordua eta/edo ordu-eremua lor dezakete. Windowseko Ordu Zerbitzuak ezartzen eta gordetzen du sistemaren ordua domeinu baten barruan, enpresa-sare bateko sistemen eta zerbitzuen arteko orduaren sinkronizazioa mantentzeko.

Collection

- T1005 – Data from Local System: Erasotzaileek sistema lokaleko iturriak bila ditzakete, hala nola fitxategi-sistemak eta konfigurazio-fitxategiak edo datu-base lokalak, iragazi aurretik artxibo interesgarriak eta datu konfidentzialak aurkitzeko. Erasotzaileek komandoen eta komando-sekuentzien interprete bat erabiliz egin dezakete hori, adibidez, “cmd” eta sareko gailuaren CLI bat. Horien bidez, informazioa biltzeko fitxategi-sistemarekin elkarri

eragiteko funtzionaltasuna dute. Erasotzaileek sistema lokalean bilketa automatizatua ere erabil dezakete.

- T1113 – Screen Capture: Erasotzaileak mahaigainaren pantaila-argazkia ateratzen saia daitezke, eragiketan zehar informazioa biltzeko. Pantaila atzitzeko funtzionaltasuna konpromisoaren ondorengo eragiketetan erabilitako urrutiko sarbide-tresna baten ezaugarri gisa sar daiteke.

Exfiltration

- T1041 - Exfiltration Over C2 Channel: Erasotzaileek datuak ebats ditzakete, aginte- eta kontrol-kanal baten bidez. Lapurtutako datuak komunikazio-kanal arruntean kodetzen dira, aginte- eta kontrol-komunikazioen protokolo bera erabiliz.

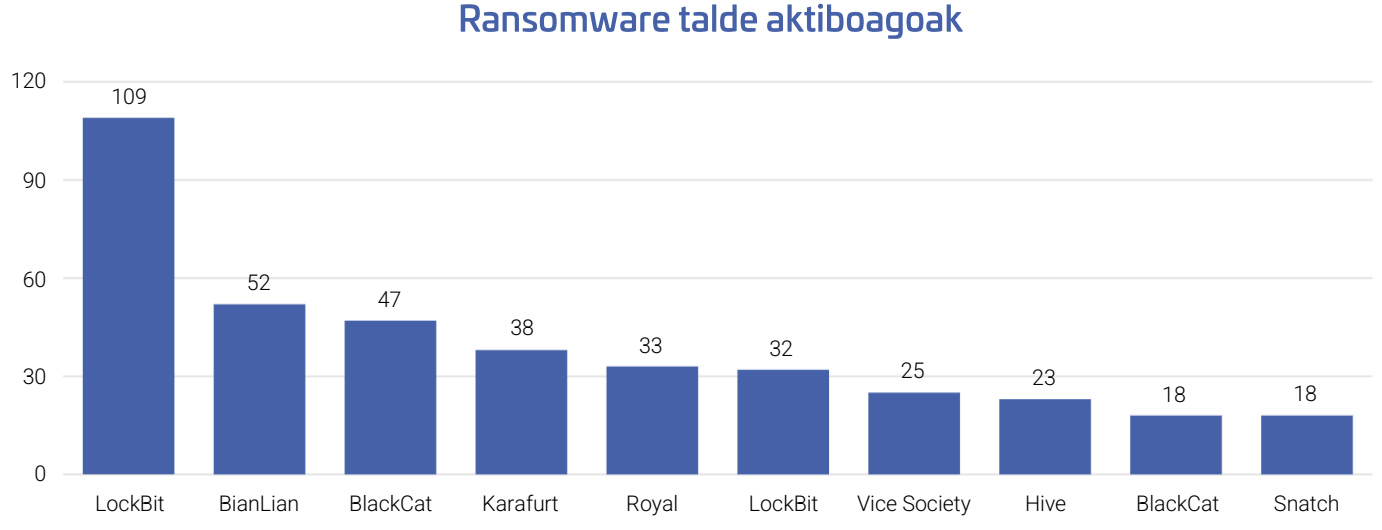
5.2. Ransomwarea

Hiruhileko honetan 390 biktima zenbatu dira guztira, ezagutzen diren ransomware talde desberdinetakoak.

Ransomwareko eragileen jardueraren laburpen gisa, hiruhileko honetan guztira 390 biktima zenbatu dira ezagutzen diren ransomware talde desberdinetan. Hurrengo grafikoan ikus daiteke Lockbit izan dela talderik aktiboena 109 biktimarekin, hau da, aurreko hiruhilekoan baino % 53 biktima gehiago izan ditu. Bian Lian eta BlackCat taldeak 52 eta 47 biktima dituzte, hurrenez hurren, eta bigarren eta hirugarren talde aktiboena da.

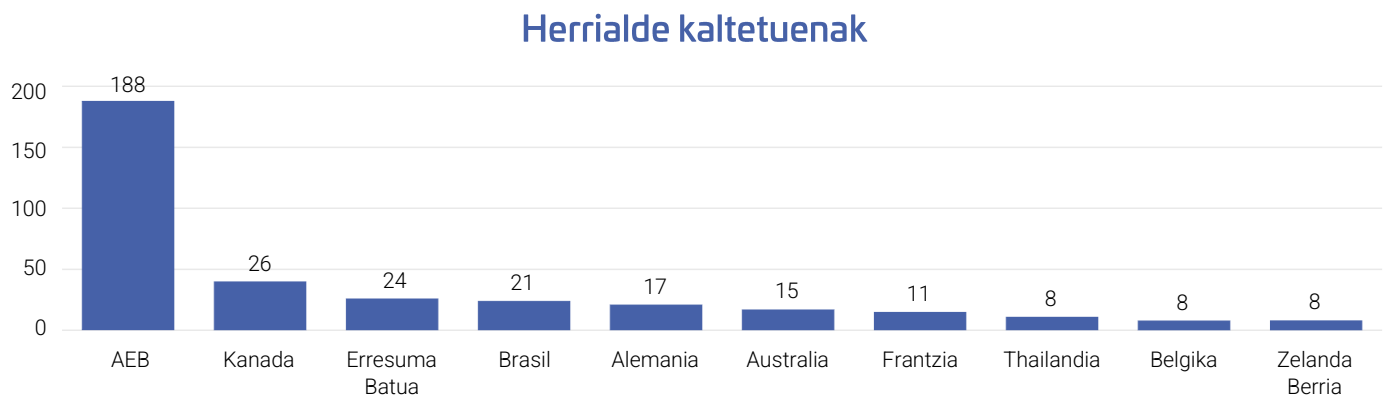
Lockbit izan da biktima gehien aitortu dituen ransomware taldea, 109 guztira.

Ransomware talde aktiboenen TOP 10 grafikoa honako hau da:



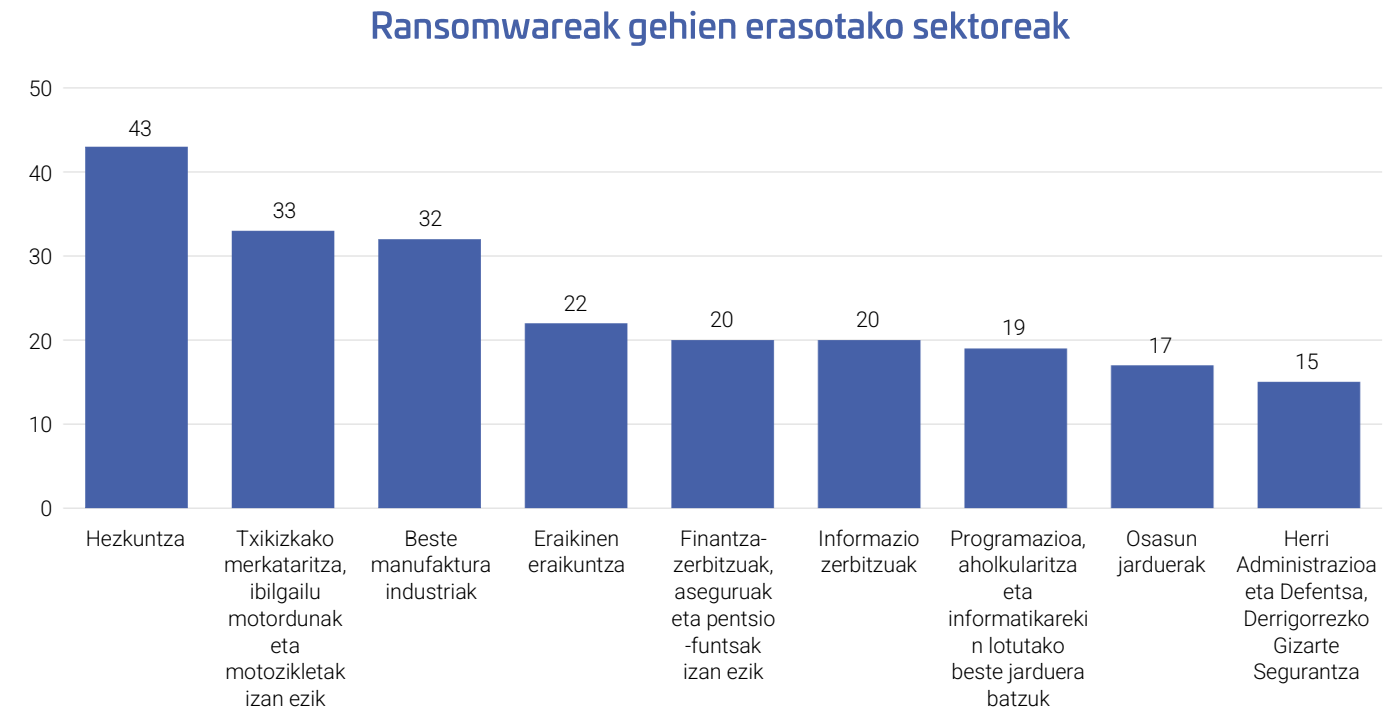
RANSOMWARE TALDE AKTIBOENEN TOP 10A. ITURRIA: BCSC.

Ransomware mota bakoitzeko herrialde kaltetuenen banaketan, Estatu Batuak dira erasotuena, ransomware mota desberdinetarako. Grafiko honetan ikus daiteke ransomware-eragile horiek gehien eragindako herrialdeen TOP 10a:



RANSOMWAREK GEHIEN ERASOTAKO HERRIALDEAK. ITURRIA: BCSC

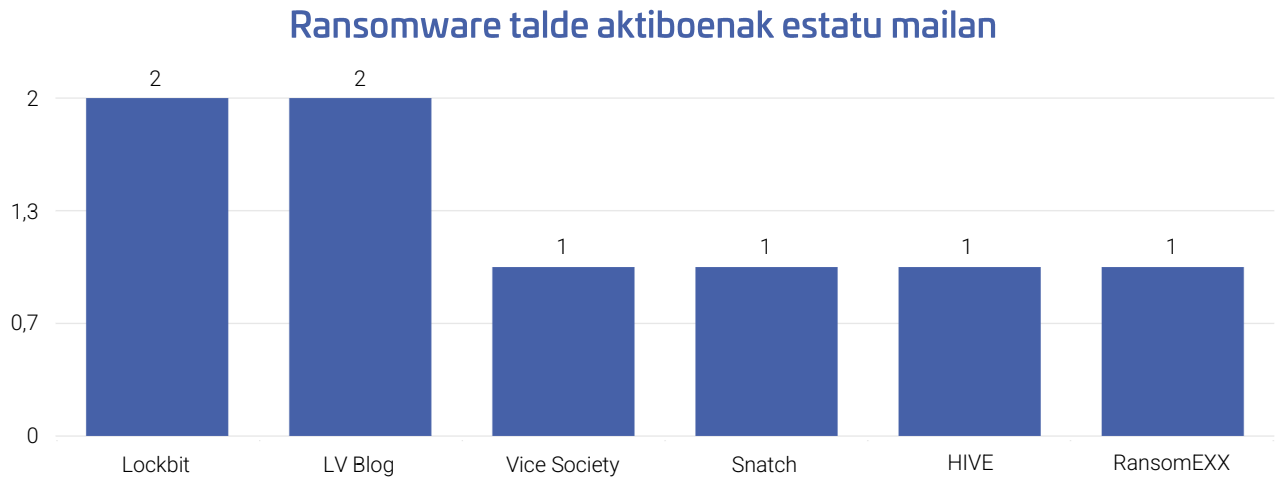
Ransomwareak gehien erasotako sektoreak aztertuz gero, ikus daiteke nazioartean gehien erasandako sektorea txikizkako merkataritzarena dela, eta, ondoren, eraikuntza-enpresena. Hezkuntzaren eta osasunaren sektorea ere eraso gehien jasan dituzten sektoreen TOP 10an dago.



RANSOMWAREAK GEHIEN ERASOTAKO SEKTOREAK. ITURRIA: BCSC

Oro har, ez da eredu bat bereizten sektore mota bati gehiago erasotzen dion jardule batetik. Kanpaina puntualak ikusi ahal izan dira, baina erasoak bereizi gabeak izaten dira.

Estatu mailan, urteko laugarren hiruhilekoan, 8 ransomware-erasoak gertatu dira, hau da, aurreko hiruhilekoan baino % 170 gehiago, orduan 10 izan baitziren. Honela banatu dira taldeen artean:

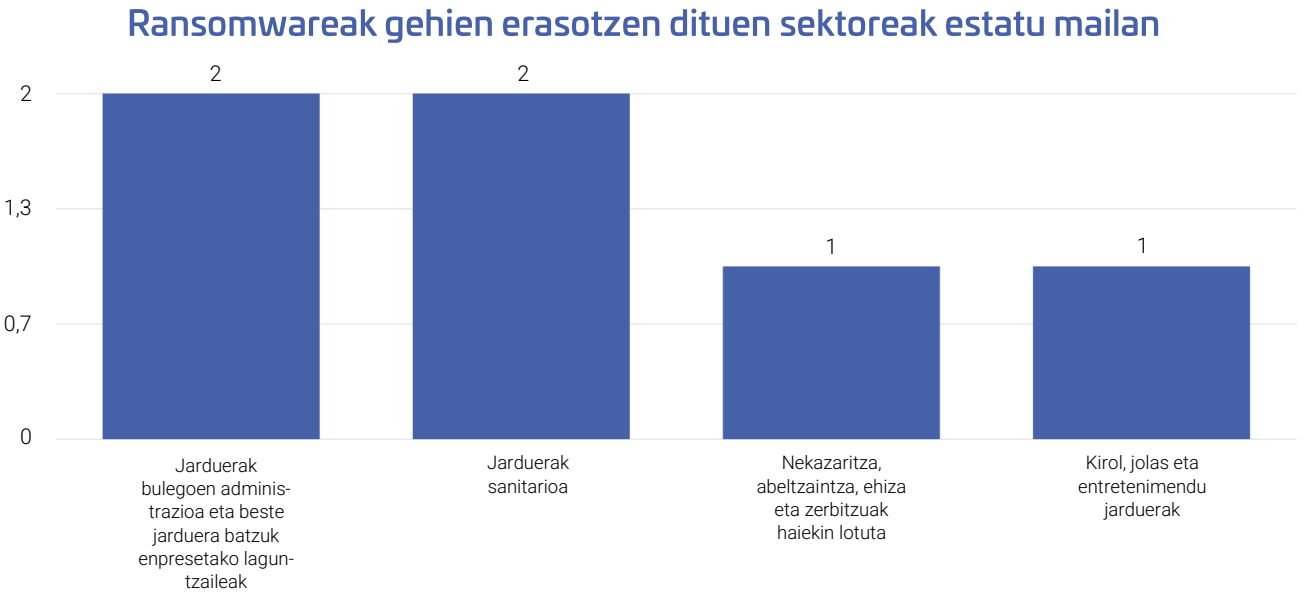


ESTATU MAILAN ERAGIN HANDIENA DUTEN RANSOMWARE TALDEAK. ITURRIA: BCSC

Garrantzitsua da kontuan hartzea datu horiek taldeek eurek argitara eman dituzten erasoetan oinarritzen direla, eta, beraz, litekeena da gehiago gertatu izana. Izan ere, zenbait ebidentzia daude erasoren bat talde horietakoren bati egotzi zaiola, baina talde horrek ez du hori aitortu bere webgunean.

Nazioartean berrikusitako joera bezala, Lockbit da intzidentzia handiena duen ransomwarea, 2 biktimarekin, LV Blogekin batera.

Gehien erasotutako sektoreei dagokienez, nahiko banatuta daude. Txikizkako merkataritza eta manufaktura-industria nabarmentzen dira, eta gainerako eraso guztiak sektore desberdin batekin identifikatzen dira, banaketa honi jarraituz:

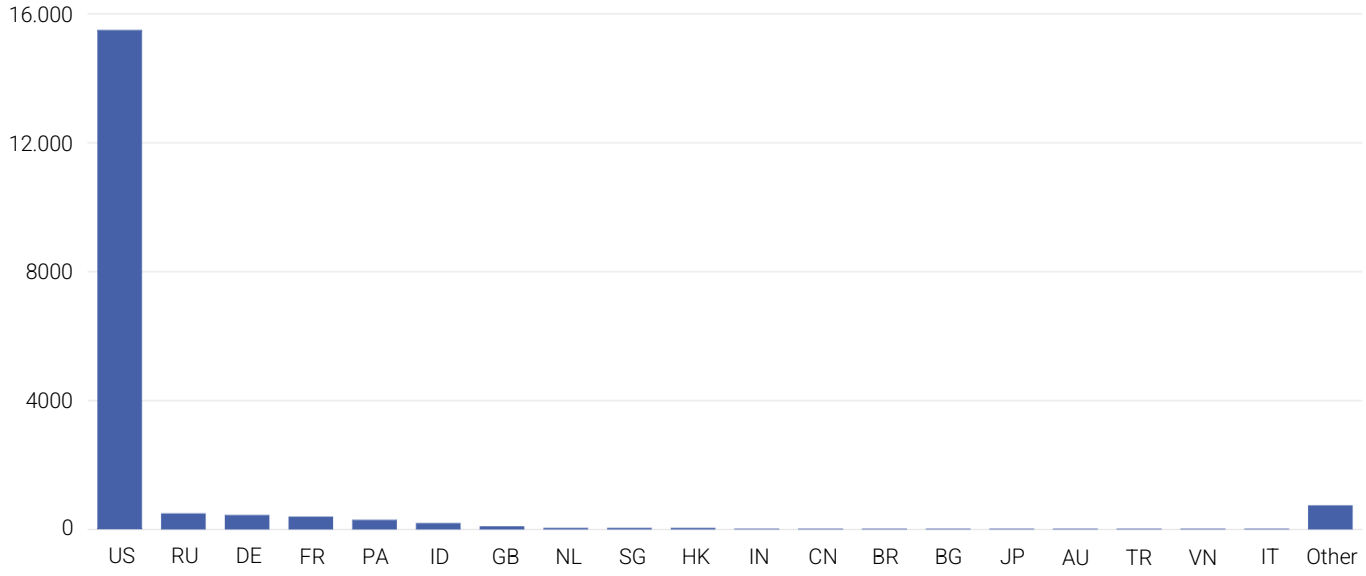


ESTATU MAILAN RANSOMWAREAK ERAGINDAKO SEKTOREAK. ITURRIA: BCSC.

6. Phishinga

Laugarren hiruhilekoan guztira 19.262 phishing URL aktibo identifikatu ditugu.

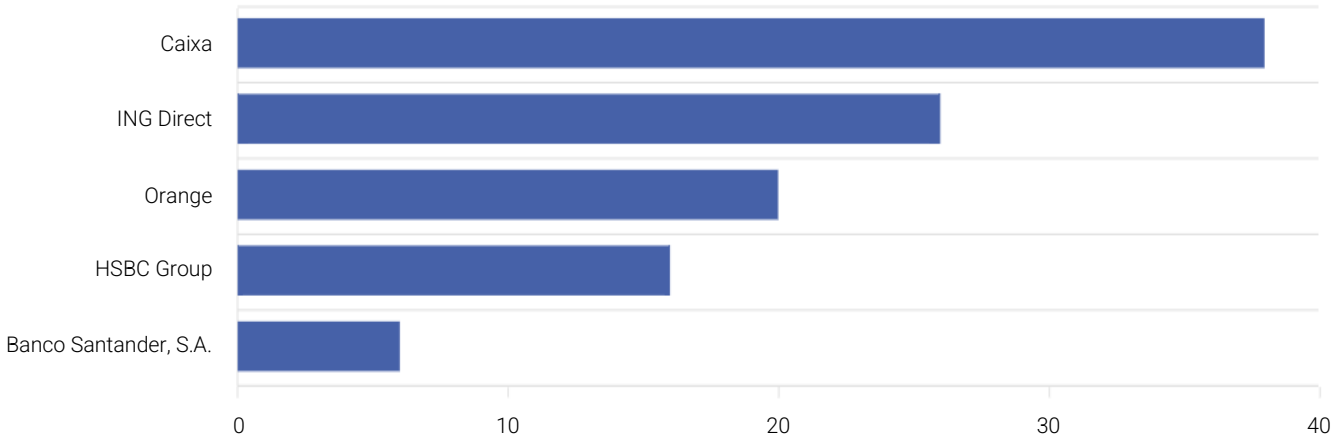
Laugarren hiruhilekoan guztira 19.262 phishing URL aktibo identifikatu ditugu. Jarraian, haien banaketa ikus dezakezu jatorrizko herrialdearen arabera:



PHISHINGAREN BANAKETA. ITURRIA: BCSC

Hiruhileko honetan phishing kanpaina gehien jasan dituzten estatuko 5 erakundeak (edo tokiko jarduera handia dutenak):

1. Caixa
2. ING Direct
3. Orange
4. HSBC Group
5. Banco Santander S.A.



PHISHINGAK ERAGIN GEIENEN ERAGILEEN ESTATU-ENTITATEEN TOP 5. ITURRIA: BCSC

7. Gomendio orokorrak

2022ko laugarren hiruhilekoan Euskadiri eragin dioten mehatxuak aztertu ondoren, arrisku ohikoenetatik babesteko landu beharko liratekeen babes-neurri egokienak identifikatu daitezke.

ATT&CK matrizeak biltzen ditu erasotzaileek Euskadin gehien erabilitako teknikak. Horri erreparatuta, honako gomendio hauek hartu behar dira kontuan:

- M1049 (Taktikak: Initial Access, Execution, Peristence, Privilege Escalation, Defense Evasion) - Erabili software maltzurra detektatzeko sistema bat.
- M1015 (Taktikak: Privilege Escalation, Credential Access, Execution, Defense Evasion) - Kudeatu sarbide -kontroleko zerrenda "Direktorio-aldaketak kopiatzeko" eta domeinu-kontrolatzailearen erreplikazioarekin lotutako beste baimen batzuk. Erabiltzaileak gehitu ditzakezu Active Directoryren "Erabiltzaile babestuak" segurtasun-taldera. Horrek erabiltzaileen testu lauko kredentzialak cachean biltegiratzea mugatzen lagun dezake.
- M1040 (Taktikak: Execution, Persistence, Persistence, Impact, Defense Evasion, Credential Access, Privilege Escalation, Initial Access) - Windows 10ean, aktibatu eraso-azalera murrizteko arauak (ASR), LSASS ziurtatzeko eta kredentzialak lapurtzea eragozteko.
- M1042 (Taktikak: Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Laeral Movement, Collection, Command and Control, Exfiltration) – Arriskutsua izan daitekeen softwarerako sarbidea ezabatzea edo ukatzea, hala nola sistema-shellak edo komando-interpreteak, erasotzaile batek erabil ez ditzan.
- M1043 (Taktikak: Persistence, Defense Evasion, Credential Access) - Windows 10en, Microsoftek "Credential Guard" izeneko babes berriak inplementatu ziren, kredentzialak iraultzeko moduen bidez kredentzialak lortzeko erabil daitezkeen LSAren sekretuak babesteko. Ez dago lehenetsita, eta hardware eta firmware sistemaren betekizunak ditu. Gainera, ez du kredentzialak lortzeko modu guztien aurka babesten.
- M1041 (Taktikak: Credential Access, Collection, Exfiltration, Impact, Defense Evasion, Credential Sniffing) - Ziurtatu domeinu-kontrolatzailearen segurtasun-kopiak behar bezala babestuta daudela.
- M1028 (Taktikak: Privilege Escalation, Discovery, Persistence, Command and Control, Exfiltration, Defense Evasion, Impact, Discovery, Lateral Movement, Execution, Credential Access) - Saiatu NTLMa desaktibatzen edo mugatzen. Hartu kontuan WDigest autentifikazioa desaktibatzeko aukera.
- M1027 (Taktikak: Credential Access, Persistance, Defense Evasion, Discovery, Lateral Movement, Execution, Exfiltration, initial Access) - Ziurtatu tokiko administratzailearen kontuek pasahitz konplexuak eta bakarrak dituztela sareko sistema guztietan.
- M1026 (Taktikak: Privilege Escalation, Persistence, Defense Evasion, Execution, Persistence, Initial Access, Lateral Movement, Impact, Credential Access, Privilege Escalation)
    - Windows: Ez sartu erabiltzaile-konturik edo administratzailearen jabari-konturik sistema guztietako tokiko administratzaile-taldeetan, oso kontrolatuta ez badaude behintzat; izan ere, sistema guztietan pasahitz bera duen tokiko administratzaile-kontu bat edukitzearen baliokidea izan ohi da hori. Jarraitu enpresa-sare bat diseinatzeko eta administratzeko jardunbide onenei, administrazio-maila guztietan kontu pribilegiatuen erabilera mugatzeko.
    - Linux: Memoriatik pasahitzak ateratzeko, root baimenak behar dira. Jarraitu kontu pribilegiatuetarako sarbidea murrizteko jardunbide egokienak, etsaien programak memoriaren zati horietara sar ez daitezen.
- M1021 (Taktikak: Initial Access, Execution, Defense Evasion, Credential Access, Lateral Movement, Command and Control, Exfiltration) - Mugatu webgune batzuen erabilera, blokeatu deskargak/fitxategi erantsiak, blokeatu Javascript, murriztu nabigatzailearen luzapenak, etab. Iragarkien bidez bidalitako kode maltzurrerako, iragarkiak blokeatzeko softwareak lehen instantzian exekutatzen lagun dezakete.

- M1025 (Taktikak: Persistence, Credential Access) - Windows 8.1 eta Windows Server 2012 R2 sistemetan, aktibatu LSArako prozesu babestuaren argia.
- M1017 (Taktikak: Credential Access, Persistence, Collection, Defense Evasion, Initial Access, Reconaissance, Execution, Credential Access) - Mugatu kontuen eta sistemen artean kredentzialak gainjartzea, erabiltzaileak eta administratzaileak informatuz hainbat kontutarako pasahitz bera erabil ez dezaten.
- M1057 (Taktikak: Collection, Exfiltration) - Datuen galeraren prebentzioak datu sentikorren bidalketa detektatu eta blokeatu dezake zifratu gabeko protokoloen bidez.
- M1031 (Taktikak: Credential Access, Command and Control, Collection, Exfiltration, Exfiltration, Lateral Movement, Discovery, Initial Access, Persistence, Defense Evasion, Execution) - Sare-sinadurak erabiltzen dituzten sare-intrusioak detektatzeko eta prebenitzeko sistemak arerioaren berariazko malware baten trafikoa identifikatzeko erabil daitezke sare mailako jarduera arintzeko. Sinadurak adierazle bakarretarako izan ohi dira protokoloen barruan, eta arerio batek edo tresna jakin batek erabiltzen duen itsukeria-teknika espezifikoan oinarritu daitezke, eta ziurrenik desberdinak izango dira hainbat familiaren eta malware-bertsioen artean. Litekeena da aurkariek tresnen Command and Control sinadurak aldatzea, edo protokoloak eraikitzea, defentsa-tresna komunek detekta ez ditzaten.
- DS0017 (Taktikak: Privilege Escalation, Discovery, Persistence, Discovery, Collection, Exfiltration, Persistence, Discovery, Credential Access, Execution, Impact, Inhibit Response Function, Defense Evasion) - Windowseko Erregistroarekin elkarri eragin diezaioketen exekutatutako komandoak eta argudioak gainbegiratzea, hala nola IP eta/edo MAC helbideak, pantaila-irudiak ateratzea edo xede-sistemetako dokumentu sentikorrak iragaztea, urruneko sistemetako informazioa aurkituz.

Basque CyberSecurity Centre

8. Bibliografia

I. https://thehackernews.com/2022/10/fbi-cisa-and-nsa-reveal-how-hackers.html

II. https://therecord.media/cyberattack-disrupts-bulgarian-government-websites-over-betrayal-to-russia/

III. https://www.noticiasdealava.eus/union-europea/2022/11/23/web-parlamento-europeo-sufre-ciberataque-6251329.html

IV. https://www.infosecurity-magazine.com/news/ransomware-australian-defence/

V. https://www.thenews.com.pk/print/1007174-indian-hackers-target-computers-of-pak-politicians-generals-report

VI. https://securityaffairs.co/138127/cyber-crime/cyberattack-blocked-trains-denmark.html

VII. https://www.europapress.es/catalunya/noticia-ciberataque-afecta-tres-hospitales-barcelona-madrugada-viernes-20221007110113.html

VIII. https://www.xataka.com/seguridad/telefonica-ha-sufrido-ciberataque-eres-cliente-movistar-u-o2-asi-puedes-cambiar-contrasena

IX. https://www.interior.gob.es/opencms/eu/detalle/articulo/La-Policia-Nacional-desarticula-una-organizacion-criminal-dedicada-al-fraude-del-CEO-que-operaba-a-nivel-nacional-e-internacional/

X. https://www.noticiasdealava.eus/sociedad/2022/11/19/ciberataque-grupo-noticias-6243829.html

XI. https://www.elcorreo.com/alava/araba/cinco-detenidos-banda-alava-por-estafar-a-clientes-entidades-bancarias-con-envio-sms-falsos-20221021104817-nt.html

Basque CyberSecurity Centre

BASQUE CYBERSECURITY CENTRE:

Zibersegurtasunaren topagunea Euskadin

El punto de encuentro de la ciberseguridad en Euskadi

info@bcsc.eus

Albert Einstein 46, 3ª planta Edificio E7
Arabako Teknologi Parkea
01510 Vitoria-Gasteiz

945 236 636