Urtarrila 2021

Ciber Eguraldia

BCSC

Albiste orokorrak

Zibersegurtasuneko gertakariak

Maulak eta iruzurrak

Malwarea eta ahultasunak

Informazio ihesak

Zibersegurtasun industriala

Albiste orokorrak

Zibersegurtasuneko inbertsioa %10 haziko da aurten

12.000 milioi eregistro baino gehiago arriskuan jarri zuen 2020an eta ransomware erasoen kopuruak ia % 60 egin zuen gora. Urrutiko lan eta ikaskuntza masiboak eta eraldaketa digitaleko proiektuen bizkortzeak joera horri eutsiko dote 2021ean.

Espainiako konpainien% 86k ez du zibersegurtasunaren kulturarik

PwC-ren azterlan baten arabera, Espainiako konpainietako zibersegurtasunaren kultura-maila 2,8 puntukoa da Setik; zibersegurtasunaren arloan kontzientziatzeko eta prestatzeko batez besteko aurrekontua informazioaren segurtasunera bideratutako guztizkoaren % 9 baino ez da eta konpainien % 11k soilik neurtzen dute arlo horretako langileen kontzientziazioa.

DarkMarket-eko arduraduna atxilotu dute, Darknet-eko merkaturik handiena, 500,000 erabiltzaile eta 2.400 saltzailerekin

Jaitsiko DarkMarket 2008an deszentratu zuten, bere sortzailea kartzelan zegoela. Merkatu berriak izena jaso zuen eta orduan izan zuena baino maila altuagoa lortu du: milioi erdi erabiltzaile baino gehiago eta 2.400 saltzaile inguru atxikoketaren unean.

Langileen segurtasuna eta erasoen prebentzioa, 2021erako erronka nagusiak

TI-ren arduradunen erdiek adierazi dute beren segurtasun-ikuspegia ez dela pandemiaren aurreko berbera izango. 2023ra arteko lehentasun nagusiak urrutiko lana, endpoint-en eta galtu mugikorren segurtasuna eta hodei publikoaren eta multikloudeen segurtasuna ziurtatzea dira.

Ziberdelituen % 88 ordainketa digitaletako iruzurrak dira

Ordainketa digitalen erabilera gero eta handiagoarekin batera, iruzurrek gora egin dute, iruzurgileek beren segurtasun-arrakala larriei etekina ateratzen dietelako. 2019an salatutako ziberdelituen % 88 ordainketa digitaletik lotutako iruzur informatikoei zegokien eta 192.000 salaketa baino gehiago izan zren.

Zibersegurtasun-gertakariak

Emotet, "munduko malwarerik arriskutsuena", suntsitu du mundu mailako polizia-ekintza batek

Nazioarteko koordinatzaileak ekintza batean, Alemania, Estatu Batuak, Erresuma Batua, Frantzia, Herbeherekak, Lituania, Kanada eta Ukrainako polizia eta kidego judizialetako ikertzaileek sarea kontrolatzen zuen azpiegitura kontrolatzea lortu dute. Guzti hori, Europol eta Eurojusten koordinazioapean, herriaklaren arteko koordinazio judizialeko organo europarraren koordinazioapean.

Segurtasun-ikertzaileen aurkako kanpaina bat abiarazi da

Googleko mehatxuen analisi-taldeak hainbat konpainiatako segurtasun-ikertzaileen aurkako kanpainaren ikerketa argitaratu zuen. Dirudienez, kanpaina 2020ko azken hilabetetean eta urtarrileko lehen astetan egingo zen. Txostenaren arabera, kanpainaren jatorria Ipar Korean egon liteke, eta segurtasun gobernuak berak babestu du.

FBIk Egregor ransomwarearen erasoei buruz ohartarazi die konpainiei mundu osoan

Komunikatuaren arabera, Ransomware Egregor, ustez 150 biktima baino gehiago dituena, informazioa lapurtzen eta artxiboak zifratzen ari da, ordoren erreskatea eskatzeko, bere helburuak lortzko taktika ezberdinak erabiliz.

Maulak eta iruzurrak

Kontuz deitzen badizute etxean COVID-19ren aurkako txertoa jarriko dizutela esanez: Guardia Zibilak "iruzur saiakera" bat dela dio

Guardia Zibilaren arabera, "bakarrik bizi diren pertsonen etxebizitzara sartzeko iruzur saiakera" izan da. Usaitako Ministerioaren arabera, dei horiek abenduaren 27an Espainian hasitako txertaketa-kanpainarekin bat datoz.

Mezu elektroniko bat jasotzen baduzu DGTaren ustezko isun batekin, ez kasurik egin!

INCIBEK iruzurrezko mezu elektronikoak bidaltzeko kanpaina bat antzeman du, Trafikoko Zuzendaritza Nagusia (DGT) ordeztu nahian, malwarea zabaltzeko asmoz. Kanpaina horretan, mezu elektroniko bat bidaltzea da, garraio- eta mezularitza-enpresa ezagun horietako baten langilea dela adierazi, eta faktura edo bidalketa-ziurtagiri batekin lotutako dokumentu bat eransten dela adierazten da, mezu elektronikoaz jasotzen duen erabiltzaileak ireki dezan.

Vodafoneren faktura eta Burofax-a online. Banku-troiarren kanpainak itzuli dira

Ekintzara itzultzean, gaizkileak ez dira gehiegi berritu; izan ere, aurreko kanpainetan jada ezagunak eta erabilak ziren posta-kantitoiek berrerabili dituzte, Vodafone telekomunikazio-enpresaren nortasuna ordezten dutenak kasu eta, hori bai, postan jasotako datak eguneratu dituzte, ortografia-akats batzuk zuzendu gabe.

"Eskaera berrestea" Posta erabiltzen dute Amazon ordezkatuz zure kreditu-txartela lortzeko

Oraingo honetan, Amazoni egindako eskaera baten berresperna simulatzen duen mezu elektroniko bat aurkituko dugu, entrega-data eta eskaera-zenbaki batekin, jasotzen duen erabiltzailearentzat sinesgarriagoa egiten saiatzeko.

18 pertsona atxilotu dituzte Bizkaian, Interneten ehun bat iruzur egiteagatik, Kantabrian ere bai

Iruzurgileak biktimekin harremanetan jartzen zren salerosketako atari ezagunen bidez eta ordaintzen ez zituzten eta ondoren saltzen zituzten produktuak saldzea adosten zuten.

Malwarea eta ahultasunak

Zero-days ahultasunak IOS-en

Applek kritika gisa katalogatutakoa zero-day motako hiru ahultasun plazaratu ditu, macOS eta IOS sistema ezagubeak erabiltzen produktuei eragiten dietenak. Lehenengoak kernelari eragiten dio, gainerako softwareak hardwarera sartzea ahalbidetzen duen sistema eragilearen funtzeetako zatiari. Beste bi ahultasunak Applek Safarirako garatutako WebKit nabigatzailearen motorrean aurkitu zuten. Fabrikatzaileak berak iOS 14.4 eta iPadOS 14.4 bertsioak lehenbailehen eguneratzeko eskatu du, akats horiek konpontzeko.

Zaurgarritasuna SUDOan

Qualys enpresako segurtasun ikertzaileek SUDO erabilgarritasunaren ahultasun kritikoaz ohartarazi dute, Unix eta Linuxen oinarritutako ia sistema eragile guztietan baitago. Programa honek root erabiltzailearen (sistemarako sarbide administratiboa duen erabiltzailea) segurtasun-pribilegioak dituzten jarraibideak exekutatzeko aukera ematen du, baldin eta pribilegioak badaude edo erabiltzaile horren pasahitza ezagutzen bada.

Zero eguneko zaurgarritasunak SonicWall-en VPN soluzioei eragiten die. Nola arindu ustiapen-arriskua?

SonicWallekoy segurtasun taldeak segurtasun alerta bat eman zuen hacker talde batekin lotuta. Talde hori sare pribatu birtualeko (VPN) ittenbidetetan zero eguneko failia bat lehertzen ariltu da eta horrek barne erasoak hedatzea ahalbidetu dezake. SonicWall-eko produktuak mota guztietako enpresa txiki eta ertainek erabiltzen dituzte eta, beraz, adituen ustez, irismen handiko arazoa da hori.

Drupaleko korearen zaurgarritasuna

Zorroztasun kritikoko urrakortasun bat argitaratu da Archive_Tar liburudendan, Drupaleko corean eragiten diona. Archive_Tar liburudendan esteka sinbolikoak behar ez bezala egiaztatuz gero, idazketa-eragiletak egin ahal izango liateke Directory Traversal enpresarekin. CVE-2020-36193 identifikatzailea esleitu da zaurgarritasun horretarako.

Microsoftek zero day eta beste 83 ahultasun zuzendu ditu urtarrileko eguneratzean

Patch Tuesday ezagunaren eldoko hontan, konpainiak produktu ezberdinetan zeuden 83 ahultasun konpondu zituen. Konpondutakoa zaurgarritasun guztietatik, 10 kritikotzat jo zren. Zuzendutako akatsetako bat Microsoft Defenderi eragiten dion zero-day bat da.

Atzeko ate bat antzeman dute 100.000 firewalls eta VPN Zyxel baino gehiagotan

Zyxel sare-ekipamenduaren fabrikatzailearen eragiten dio eta haren softwarearen kodearen barruan "hardkodedun" kredentzialak (arg idatzita) filtratuko liateke eta besteen esku jarriko liuzkete, potentzialki, 100.000 gailu edo gehiago.

Pribatutasuna eta informazio ihesak

Zaurgarritasuna aurkitzen dute Tiktoken eta agerian uzten ditu telefono-zenbakia eta erabiltzaile-profilen informazioa

Hain zuzen ere, , konpainiak azaldu duenez , akatsa "lagunak aurkitzeko" funtzioan legoke eta zibergaizkileei erabiltzaileen profilaren informazioa eskuratzeko aukera emango leke. Telefono-zenbakia, izena, profilaren argazkia, abatarra, identifikazio bakarrak eta profilaren konfigurazioa barne hartzen ditu.

Datuak Babesteko Agentziak Caixabanki jarritako isuna: 6 milioi euro, datu pertsonalen lagapena behartzeagatik

Datuak Babesteko Espainiako Agentziak inoiz jarritako isunik handiena da, 6 milioi eurokoa. BBVA ziguriru eta hilabetera, datuak bidegabe erabiltzeareakin lotutako hainbat isun jarri zion Caixabanki.

Ubiquitik pasahitzaren aldaketa eskatu du, datu-filtrazio baten bidez

Horren arrazoia, kanpoko hodei horretatik baten kokatutako sistemek eraso batzuen erasoa da. Horren ondorioz, erabiltzaileen datuak iragazi ahal izan dira eta horregatik,oso garrantzitsua da gakoak berehala aldatzea eta arazo handiagoak saihestea.

Zibersegurtasun industriala

Zibergaizkileek txertoen aurkako erasoen maiztasuna handitzearen benetako arrazoiak

Zibergaizkileak beren eraso informatikoak koronabirusaren aurkako botikak amaitzen dituzten farmazialarirangan zentratzen hasiak zren. Baita hotz-kateen aurka ere, dosi askoren banaketa bermatzeko ezinbestekoak diren azpiegitura logistikoak baitira.