ZIBERDELITUGILEAK KORONABIRUSA BALIATZEN ARI DIRA BEREN JARDUERARI EUSTEKO

- **Azken asteotan esponentzialki handitu da COVID-19a aitzakiatzat erabiltzen duten zibermehatxuen kopurua.**
- **Mehatxu horien aurrean babesgabe ez egoteko funtsezkoa da modu egokian jardutea.**

Ziberdelitugileek etengabe bilatzen dituzte erabiltzaileen segurtasuna kolokan jarriz etekin ekonomikoa lortzeko moduak. Honenbestez, azken asteetan COVID-19 pandemiak eragindako zorigaitzaz baliatzen ari dira beren jarduera makurretarako. Koronabirusa globalki hedatzen hasi ahala, egoera horri etekina atera nahi dioten ziberkriminalen ekintzak ere ugaritu ziren. Azken asteotan behatu dugunez, gora egin dute phishingak, era guztietako iruzurrek eta COVID-19a aitzakiatzat erabiltzen duten programa gaiztoek. Era berean, koronabirusarekin zerikusia duten eta aipatutako helburuetarako erabiltzen diren domeinuen erregistroak ere goraka doaz.

Hainbat eratakoak dira ziberdelitugileen ekintzak

Ondoren aipatuko ditugun adibideak ez dira bakarrak, baina ederki adierazten dute zein motatako ekintza gaiztoak gauzatzen dituzten ziberkriminalek, COVID-19a baliatuta.

Urtarrila iritsi orduko, Txinako krisi betean, **phising eta malware-zabalkunde** kasuak hasi ziren. EMOTET eta Lokibot banku-troiarrak hedatu ziren Txinako Osasun Ministerioa ordezten omen zuten posta elektronikoko mezuen bidez. AZORult ere zabaldu zen, Microsoft Officeko fitxategia bailitzan, kutsatutako ordenagailuan kode gaiztoa exekutatzeko aukera ematen zuen CVE-2017-11882 ahulgunea aprobetxatuta. Eta azkenaldiko berrien arabera enpresak eta gobernu-erakundeak jomuga dituen phishing-kanpaina bat dago martxan, informazio labaina lortzeko asmoz fitxategi erantsi bat igortzen duen posta elektronikoko mezuak bidaltzen dituena.

Ugari ditugu **telefono mugikorren aurkako mehatxuak** ere, Android gailuen aurkakoak bereziki. Zehazki, CovidLock ransomwarea, itxuraz COVID-19ari buruzko informazioa bilatzeko aplikazioa, telefonoak blokeatzeko erabiltzen da, erreskate bat ordaindu arte.

info@bcsc.eus | 945 010 059

Arabako Teknologia Parkea
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz

BASQUE CYBERSECURITY CENTRE
GRUPO spri TALDEA
EUSKO JAURLARITZA GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Antolatutako ziberdelitugile-taldeen erasoaldi gidatuak ere atzeman dira, “Mehatxu Iraunkor Aurreratuak” izenekoak (“**Advanced Persistent Threats” – APTs**, ingelesez). Horietan, gaizkileak Osasunaren Mundu Erakundea (OME) ordezkatzen saiatu dira, informazio labaina eskuratzeko xedez. Hades APT izan da aktiboenetako bat, Mustang Pandak ustez Vietnamgo Lehen Ministroak egindako adierazpenak erakusten zituen eta “Vicious Panda” malwarea zuten mezuak zabaldu ditu, eta Libian beste talde bat dabil informazio labaina bildu nahian spywarea erabiltzen, koronabirusari buruzko SpyMax app-ean ezkutatutako malwarea hedatuz; horri esker dei-zerrenda eta testu bidezko mezuak lor ditzakete, baita telefonoaren kamera edo mikrofonoa aktibatu ere.

Oihartzun handia izan du, halaber, Osasunaren Mundu Erakundea (OME) ordezkatzeko kanpaina batek. Bitcoin bidez egin beharreko dohaintza bat eskatzen zuen, COVID-19rako sendagai bat bilatzeko ikerketari laguntzeko.

Herrialde askotan, konfinamendua dela eta **telelana** egin beharra VPN faltsuak sortzeko baliatzen ari da, haien bidez datuak lapurtzeko, pertsonalak zein enpresenak.

Hainbat eratako **web bidezko iruzurrak** ere ugaritzen ari dira: birusaren proba egiteko kitak, dohaintzak jasotzeko webgune iruzurtiak, edo Darkneteko merkatuetan askotariko produktuak eskaintzen eta saltzen dituzten atariak.

Estortsio-kasuek ospitaleei ere eragiten diete, eta jakina da Txekiar Errepublikako ospitale batek, behintzat, halako eraso bat jasan duela. Ziberdelitugile-talde ugarik “adierazi” badute ere ez zitzaiela erasorik egingo medikuntzako instalazioei edo osasunarekin zerikusia dutenei, APT MAZE taldeak Erresuma Batuko instalazio bateko datu konfidentzialak filtratu zituen, hark erreskate bat ordaintzeari uko egin eta gero.

Bestalde, erabiltzaileen **datuen pribatutasuna** ere eztabaidagai da, frogatu baita COVID-19aren aurka borrokatzeko sortutako aplikazioetako batzuk zibersegurtasuna kontuan hartu gabe garatu direla, eta horren ondorioz ahulguneak dituztela, edo areago, biltzen duten informazioa modu “zalantzazkoan” erabiltzen dutela. Era berean, frogatu da herrialde batzuk, infekzioa kontrolatzeko asmoz, hasita daudela beren herritarren kokapena behatzen, eta hainbat enpresa handi, hola nola Facebook, Apple, Amazon eta Google, besteak beste, informazioa sortzen ari direla beren langileen kokapenaz, solaskideez, ohiturez etab.

Kontzientziazioa eta zuhurtzia, segurtasun-aholku onenak

Beste alde batetik, asko ugaritu dira **albiste faltsuak (fake news)**, sare sozialen eta posta elektronikoaren bitartez batez ere. Jokabide egokiena dena xehe-xehe aztertzea da, eta benetako sinesgarritasuna duten enpresez, pertsonez eta erakundeez besterik ez fidatzea, baita tokiko zein nazioetako gobernuen agentziez ere.

Pandemiari beldurraren eraginez, erabiltzaile zuhurrenak ere bihur litezke iruzurgileen eta ziberdelitugileen helburu, arriskuak aintzat ez hartzeagatik. Ezinbestean, kontzientziatu egin behar dugu ustez legitimoa den iturri batetik etorri zaigun mezu elektronikoak programa gaiztoren bat (malware) izan dezakeela, eta ondo pentsatu behar dugula erantsitako fitxategiak irekiko ditugun ala ez.

Azkenik, enpresek **beren langileen eta haiek darabiltzaten datuen segurtasuna bermatu** behar dute, urruneko lana egiten denean. Jarduera modu seguruan egiten laguntzeko politikak ezarri behar dira: VPNa erabiltzea, pasahitz sendoak izatea, softwarea eguneratzea, gailuak arduraz erabiltzea, etab.

Datuak babesten laguntzeko asmoz, koronabirusari buruzko berariazko orri bat sortu dugu. Bertan argitaratuko ditugu zibermehatxuei aurrean jokatzen lagunduko duten hainbat dokumentu.

info@bcsc.eus | 945 010 059

Arabako Teknologia Parkea
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz