Mondragon Unibertsitatea

Biblioteka

Konpetentzia digitalak

Graduko ikasleentzako formakuntza materialak

4. Segurtasuna

4.1. Gailuen babesa:

4.1.1. Ingurune digitaleko mehatxuak

CRUE-REBIUNek egindako eta Mondragon Unibertsitateko Bibliotekak moldatutako materiala

Segurtasuna.
Gailuen babesa.

INGURUNE DIGITALEKO MEHATXUAK

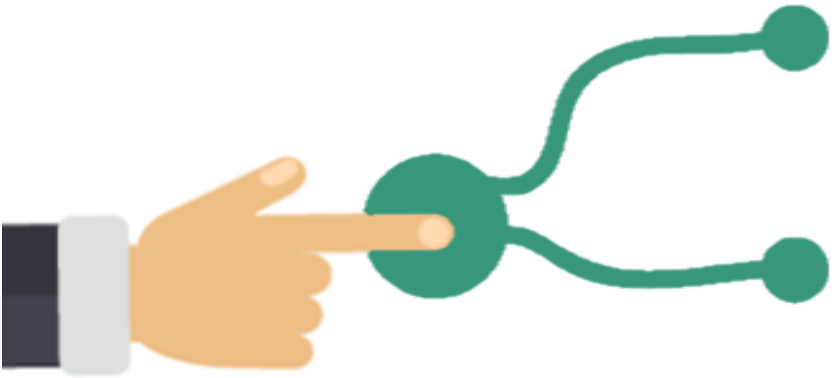
CRUE REBIUN
Red de Bibliotecas Universitarias

LABURPENA

- Segurtasun-mehatxuak linean
- Malware
  - Birusa
  - Zizarea
  - Spyware
  - Adware
  - Ransomware
  - Troiatarra
- Phishing
- Botnet
- Spam

HELBURUAK

Jarduera hau egin ondoren, gaitasun hauek lortu behar zenituzke:



Software gaiztoaren eta bestelako mehatxuen ezaugarriak eta arriskuak ezagutzea

Mehatxuek linean nola jarduten duten eta nola detektatzen diren ikastea

SEGURTASUN-MEHATXUAK LINEAN

Gure gailuak sarera konektatzen ditugun unetik, mehatxu eta arrisku askoren eraginpean gaude; **zibermehatxuak** ere deitzen zaie, eta segurtasun-ahultasunak aprobetxatzen dituzte ekipoei eraso egiteko.

Zibergaizkileek etengabe hobetzen dituzte eraso-metodoak, segurtasun-tresnei iskin egin ahal izateko; beraz, komenigarriena kontziente izatea eta gailuak babesteko behar diren neurriak hartzea da.

Hauek dira gailu pertsonalen mehatxu nagusiak:

- Malware
- Phishing
- Botnet
- Spam

Segurtasun-arriskuek konektaturik dagoen edozein gailuri eragiten diote: ordenagailuei, gailu mugikorrei edo konektatutako objektuei, hala nola etxetresna elektriko, bonbila, bozgorailu, eta abarri.

MEHATXUAK: MALWARE

TIPOS DE MALWARE

Malwarerik ezagunenak gure gailuak kutsatzeko eta hedatzeko erabiltzen direnak dira:

- Birusa
- Zizarea

Beste malware-mota batzuek gure datu pertsonalak lapurtu edo publizitate-baztergarriaren bidez etekinak lortu nahi dituzte:

- Spyware
- Adware

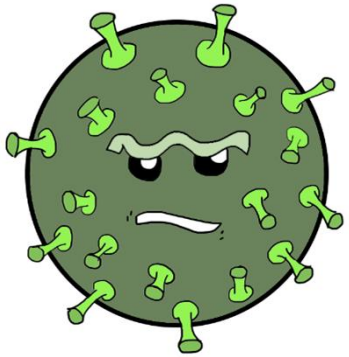
Malware-mota sofistikatuago batek gailuak baliogabetu ditzake ekipoak blokeatuz edo edukia zifratuz:

- Ransomware

Gainera, hainbat motatakoa izan daitekeen malware ezkutu bat ere bada:

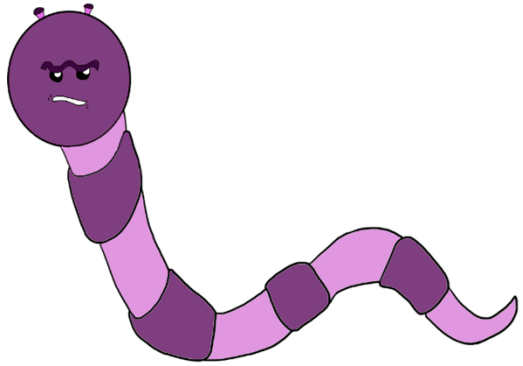
- Troiatarra

MEHATXUAK : MALWARE - BIRUSA



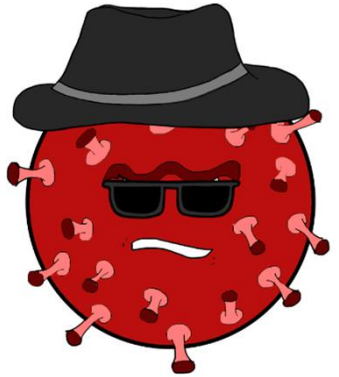
BIRUSA	
Zer da?	Gailu batean baimenik edo ezagutzarik gabe exekutatzen den kode gaiztoa duen programa edo zatia.
Nola iristen da gailuetara?	Software bat exekutatzean, web orri baten bidez edo posta elektronikoko eranskin gisa lortutako fitxategi ustel bat irekitzean instalatzen da.
Nola jarduten du?	**Fitxategiak eta karpetak kutsatzen ditu**, bere burua errepikatuz, erabiltzaileak jakin gabe, eta datuak nahiz aplikazioak aldatu edo ezabatzera iristen da. Gailua erabat infektatzea eta haren kodea Internet bidez edo USB memoriak bezalako beste gailu batzuen bidez hedatzea du helburu.
Nola saihesten da?	Honakoak saihestu behar dira: iturri ezezagunetatik programak edo aplikazioak instalatzea, fitxategi ez-fidagarriak deskargatzea, edo postako igorle susmagarri edo ezezagunen eranskinak irekitzea.
Nola antzematen da?	Gailua motel bihur daiteke. Aplikazioaren portaera irregularra da. Interneteko konexioa ezegonkorra izan daiteke. Detekzio programak desgaitu egin daitezke.
Nola kentzen da?	**Antibirusa** edo malware aurkako tresnekin.

MEHATXUAK: MALWARE - ZIZAREA



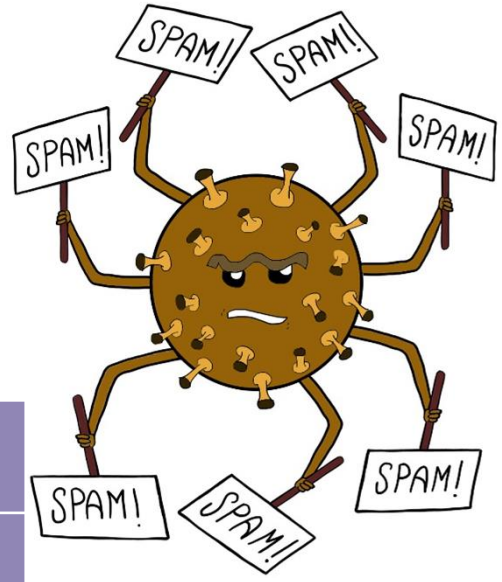
ZIZAREA	
Zer da?	Gure baimenik edo ezagutzarik gabe gailu batean exekutatzen den programa gaiztoa.
Nola iristen da gailuetara?	Web orri baten bidez edo posta elektronikoaren eranskin gisa lortutako fitxategi ustel bat irekitzean instalatzen da.
Nola jarduten du?	Bere helburu nagusia jatorrizko gailu baten barruan **autoerreplikatzea** eta sarean zehar **hedatzea** da. Birusak ez bezala, ez du erabiltzailearen exekutazio beharrik. Normalean, barne-memoria ugari eta sareko datu asko kontsumitzen ditu. Ez du kalte larririk eragiten artxibo edo gailuetan, baina haien jarduerak blokea ditzake.
Nola saihesten da?	Honakoak saihestu behar dira: iturri ezezagunetatik programak edo aplikazioak instalatzea, fitxategi ez-fidagarriak deskargatzea, edo postako igorle susmagarri edo ezezagunen eranskinak irekitzea.
Nola antzematen da?	Gailua moteldu daiteke blokeatzeko arriskuarekin. Interneteko konexioa ezegonkorra izan daiteke. Sareko datuen **kontsumoa** izugarri igo daiteke.
Nola kentzen da?	**Antibirusa** edo malware aurkako tresnekin.

MEHATXUAK: MALWARE- SPYWARE



SPYWARE (ESPIA PROGRAMA)	
Zer da?	Gailu bat baimenik gabe edo erabiltzaileak jakin gabe kontrolatzeko diseinatutako kode gaiztoa duen programa edo zatia.
Nola iristen da gailuetara?	Software bat exekutatzean edo mezu elektronikoari erantsitako fitxategi ustel bat irekitzean instalatzen da. Baita aplikazio edo web orri batetik ateratzen den publizitate baztergarriko iragarkietan sartzean ere.
Nola jarduten du?	Automatikoki instalatzen da eta gailua piztuta dagoen bitartean jarduten du. Datu pertsonalak, nabigazio-historia, kokapena, pasahitzak edo bankuko **datuak biltzen ditu.** Batzuetan, nahi ez duzun publizitatea bistara dezake.
Nola saihesten da?	Honakoak saihestu behar dira: programak edo aplikazioak iturri ezezagunetatik instalatzea, gailuko edo nabigatzaileko leiho berrien oharrak onartzea, publizitate baztergarria irekitzea edo posta igorle susmagarri edo ezezagunen eranskinak irekitzea.
Nola antzematen da?	Gailua moteldu dezake blokeatzeko arriskuarekin. Erabiltzaileak instalatu gabeko aplikazio berrien ikonoak agertuko dira. Nabigatzailearen hasierako orria ez da ohikoa izango. Ohikoak ez diren errore-mezuak eta nahi ez diren publizitate abisuak agertzen dira.
Nola kentzen da?	Antibirusa edo **spyware-aren aurkako tresnekin.** Windows-ekin lan egiten duten ekipoetan Firewall aktibatuz. Nabigatzailean leiho berrien blokeatzaile bat instalatuz. Gainera, aplikazio susmagarriak desinstalatzea gomendatzen da.

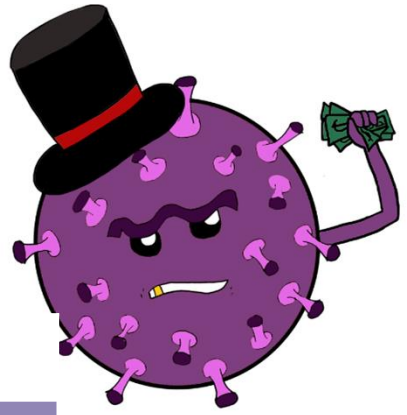
MEHATXUAK: MALWARE - ADWARE



ADWARE (PUBLIZITATEDUN PROGRAMA)

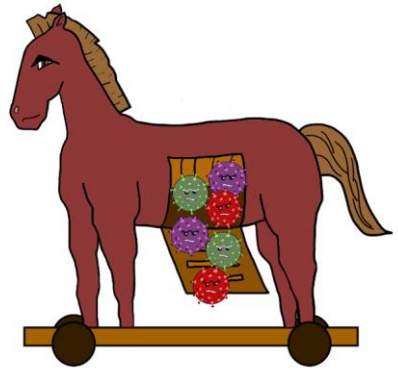
Zer da?	Nahi ez den publizitatea erakusteko diseinatutako programa. Oro har, soilik gogaikarria da, baina bertsioetako batzuk spyware gisa joka dezakete.
Nola iristen da gailuetara?	Barruan dakarren software bat exekutatzean instalatzen da. Baita, aplikazio edo web orri batetik ateratako publizitate baztergarriko iragarki batera sartzean ere.
Nola jarduten du?	Aplikazio edo web-orrietatik ateratzen **publizitate baztergarriko iragarkiak** leiho berriak irekitzen ditu. Batzuetan, datu pertsonalak, nabigazio-historiala edo kokalekuaren inguruko datuak bil ditzake.
Nola saihesten da?	Honakoak saihestu behar dira: iturri ezezagunetatik programak edo aplikazioak instalatzea, gailuan edo nabigatzailean agertzen diren leihoen oharrak onartzea, nahi ez diren iragarkiak irekitzea.
Nola antzematen da?	Publizitate baztergarriko iragarkiak dituzten leiho berriak agertzen dira. Nabigatzailearen hasierako orria ez da ohikoa.
Nola kentzen da?	**Antibirusa** edo adwarea ezabatzeko tresnekin. Gailuaren sistema eragilea eguneratzen. Windows erabiltzen duten ekipoetan Firewall aktibatzen. Nabigatzailean leiho berrien blokeatzaile bat instalatuz.

MEHATXUAK:
MALWARE - RANSOMWARE



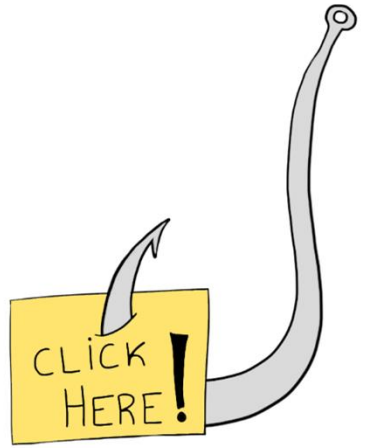
RANSOMWARE (ERRESKATE PROGRAMA)	
Zer da?	Gailu batean baimenik edo ezagutzarik gabe exekutatzen den kode gaiztoa duen programa edo zatia.
Nola iristen da gailuetara?	Software bat exekutatzean, web orri baten bidez edo posta elektronikoaren eranskin gisa lortutako fitxategi ustel bat irekitzean instalatzen da.
Nola jarduten du?	Gailua blokeatu egiten du, eta normalean, poliziaren edo FBIaren identitatea ordezkatuz ohartarazpen-mezu bat bistaratzen du. Bertsiorik beldurgarrienean, gailuaren eduki guztia zifratzen du, artxibo eta karpetetara sartzea eragotziz, eta diru-erreskate bat eskatzen du sarbidea berreskuratzeko.
Nola saihesten da?	Honakoak saihestu behar dira: gailuko edo nabigatzaileko leiho berrien oharrak onartzea, nahi ez diren iragarkiak irekitzea edo bidaltzaile susmagarri edo ezezagunen eranskinak irekitzea. Gailuaren edukiaren **segurtasun-kopiak** egitea gomendatzen da.
Nola antzematen da?	Abisuak daramatzaten leiho berriak agertzen dira poliziaren identitatea ordezkatuz. Ezin da gailuko fitxategi edo aplikazioetara sartu. Artxiboengatik erreskatea eskatzen duten mezuak agertzen dira.
Nola kentzen da?	Gaur egun ez dago modu eraginkorrean ezabatzeko gai den tresnarik. Gailua hasierako fabrikako egoerara itzultzea eta segurtasun-kopia bat leheneratzea gomendatzen da.

MEHATXUAK:
MALWARE - TROIATARRAK



TROIATARRA	
Zer da?	Itxura erabilgarri eta legitimoko programa izanik, emandako pribilegioez baliatzen da segurtasun-metodoei ihes egiteko eta ekintza gaiztoak ezkutuan burutzeko.
Nola iristen da gailuetara?	Itxuraz legitimoa den software bat instalatzean sartzen da gailuetan, ezkutuan darama kode gaiztoa.
Nola jarduten du?	**Erabilgarria dela simulatzen** du, baina malwarea birus edo spyware-a exekutatzen du. Ez du bere burua erreplikatzen, baina behin aktibatuta, gailura urrunetik sartzeko aukera ematen du. Segurtasun-eten bat sortzen da, eta horrek datu pertsonalak lapurtzea, fitxategiak ezabatzea edo gailua blokeatzea ekar dezake.
Nola saihesteen da?	Honakoak saihestu behar dira: iturri ezezagunetatik programak edo aplikazioak instalatzea, fidagarriak ez diren fitxategi exekutagarriak (.exe, .vbs, .bat luzapenak) deskargatzea, edo exekutagarriak dituzten posta-igorle susmagarri edo ezezagunen eranskinak irekitzea.
Nola antzematen da?	Gailua moteldu egin daiteke blokeatzera iritsi arte.
Nola kentzen da?	**Antibirusa** edo malware aurkako tresnekin. Gainera, aplikazio susmagarriak desinstalatzea gomendatzen da.

MEHATXUAK: PHISHING-A

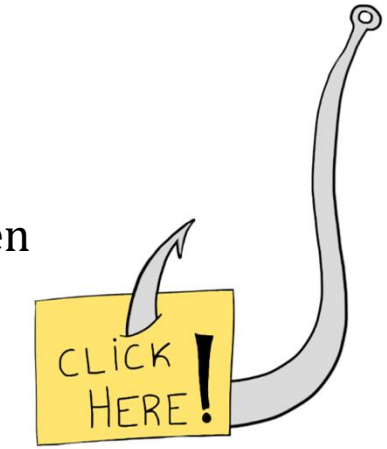


Phishing-a edo **identitate-ordezkapena** zibergaizkileek datu pertsonalak, sarbide-pasahitzak edo kreditu-txartelen datuak lortzeko erabiltzen duten engainu-modu bat da.

Posta elektroniko, SMS edo nabigatzailean agertzen den leiho baten bidez, gobernu-erakundeak, pakete-zerbitzuak, banku-erakundeak edo sare sozialak ordezkatzen dira. Mezu horiek, datu pertsonalak ematera eramaten gaituzte, eta jatorrizko webguneak xehetasun guztiekin imitatzen dituzten web-orrietara bideratzen gaituzte.

Normalean, horrelako mezuak posta edo mezularitza hornitzaileek automatikoki detektatzen dituzte baina erne egotea komeni da.

MEHATXUAK: PHISHING-A



Horrelako mezuak jasotzen direnean, garrantzitsua da **zentzuduna izatea** eta phising-saiakera baten **susmoa** izatea.

Identitate-ordezkapen baten aurrean gaudela jakiteko, garrantzitsua da:

- Datu pertsonalak, bankuko datuak edo pasahitzak eskatzen dizkiguten ustekabeko mezuak ezabatzea.
- Akats gramatikalak edo ortografikoak dituzten postak zalantzan jartzea.
- Mezu inpertsonalekin ez fidatzea: ‘Kaixo’, ‘Bezero agurgarria’, ‘Lagun agurgarria’.
- Mezuan dagoen estekara sartuz gero, egiaztatu bidali dizuten orriaren URLa; izan ere, gaizki idatzita egon ohi da, beste domeinu batean amaitu (adibidez: .ly .es beharrean) edo erabat ulertezina izan ohi baita.

Phising kasu baten aurrean gaudela susmatzen badugu, garrantzitsua da erakunde faltsutuari eta eskumena duten agintariei jakinaraztea.

MEHATXUAK: BOTNET

Bot edo botnet sare bat malware batez kutsatutako gailuen sare bat da. Malwareak, erabiltzailearen baimenik edo ezagutzarik gabe ekintza gaiztoak egiteko biltzen ditu.

Sare hauek **zombi sareak** bezala ezagutzen dira, ehunka gailu kontrolatzen dituzte *zerbitzu-ukapenaren eraso banatuetan* (DDoS) erabiltzeko, birusak zabaltzeko edo spama bidaltzeko.

Gure ekipoa botnet batean erabiltzen ari dela susma dezakegu, malwarea detektatzeko erabiltzen ditugun antzeko arrazoiengatik:

- Gailua moteldu daiteke blokeatu arte.
- Datu-kontsumoa izugarri igo daiteke.
- Gailuak etenaldi edo itxarote modutik ateratzen dira etengabe.

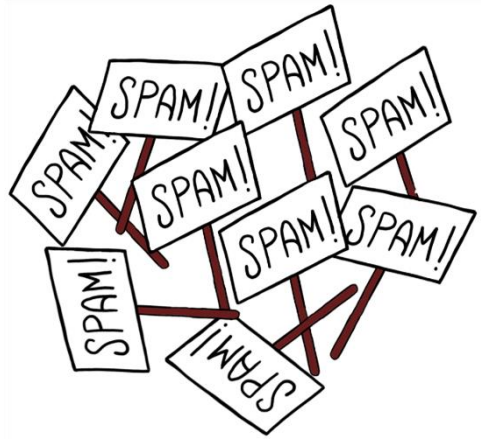
Gure ekipoen urruneko erabilera saihesteko, gomendagarria da:

- Iturri ezezagunetatik datozen programak edo aplikazioak ez instalatzea.
- Fidagarriak ez diren fitxategiak ez deskargatzea.
- Posta-bidaltzaile susmagarri edo ezezagunen eranskinik ez irekitzea.

Gure ekipoa bot-saretik ezabatzeko, beharrezkoa da antibirus edo malware aurkako-tresna bat erabiltzea.

Internautaren Segurtasun Bulegoak (OSI) tresna bat eskaintzen du gure gailua botnet batek hartu duen egiaztatzeko.

MEHATXUAK: SPAM-A



Zabor-posta, normalean **spam** gisa ezagutzen dena, publizitatea erakusten duten eskatu gabeko mezuak dira erabiltzailearen baimenik gabe, automatikoki, masiboki eta ausaz bidaliak.

Normalean posta elektronikoaren zerbitzuarekin lotuta egoten da, baina web soziala iritsi zenetik, ohikoa da nahi ez diren mezu horiek SMS, berehalako mezularitza edo sare sozialen bidez ere iristea.

Mehatxu horren helburu nagusia produktu edo zerbitzu bat saltzea izaten da, baina, batzuetan, existitzen ez diren erakundeen edo partikularren mezuak izaten dira, malware erantsi edo phishing bidez hartzailea engainatu nahi dutenak.

Posta elektronikoko edo berehalako mezularitzako zerbitzuek horrelako mezuak automatikoki iragazi eta karpeta zehatzetara desbideratzen dituzten sistemak dituzte.

Neurri horien osagarri gisa, honakoa gomendatzen da:

- Posta-kontua edo telefono-zenbaki nagusia harpidetza-zerbitzuetarako edo newsletter-etarako ez erabiltzea
- Bidaltzaile susmagarri edo ezezaguna iruditzen zaigun mezurik ez ireki eta ez erantzutea
- Spam gisa sailkatutako mezuak ez irekitzea eta ez erantzutea
- Iragazki automatikoei iskin egitea lortu duten mezu baztergarri guztiak Spam gisa kategorizatzea
- Posta-iragazki pertsonalizatuak sortzea

GEHIAGO JAKITEKO...

Eman begirada bat artikulu hauei:

Ponte al día con los virus informáticos

Qué es una botnet o una red zombi de ordenadores

Mondragon Unibertsitatea

Biblioteka

Zalantzarik baduzu, galdetu zure bibliotekan:

Basque Culinary Center
Biblioteka
Juan Abelino Barriola pasealekua, 101
20009, Donostia, Gipuzkoa.
T. 943574514
biblioteca@bculinary.com

Enpresa Zientzien Fakultatea
Biblioteka
Ibarra Zelaia, 2
20560, Oñati, Gipuzkoa.
T. 943718009
biblioteka.enpresagintza@mondragon.edu

Humanitate eta Hezkuntza Zientzien Fakultatea

Biblioteka

Dorleta, z/g.

20540, Eskoriatza, Gipuzkoa.

T. 943714157

biblioteka.huhezi@mondragon.edu

Goi Eskola Politeknikoa
Biblioteka
Campus Iturripe. Loramendi, 4. 20500 Arrasate – Mondragon, Gipuzkoa.
Campus Orona Ideo. Fundazioa eraikuntza, Jauregi Bailara, z/g. 20120 Hernani, Gipuzkoa.
T. 943794700
biblioteka.mgep@mondragon.edu