Octubre de 2019

Has patit un atac ?

- Revisar tots els equips de la xarxa i els servidors amb eines de diagnosi adequades.
- Aïllar qualsevol equip sospitós.
- Posa una denúncia, t'han robat informació confidencial.
- Comunica-ho a l'Agència de Protecció de Dades
- Avisa als teus contactes dels correus afectats.
- Sempre utilitza CCO (Còpia oculta) en els correus massius.
- Comunica-ho i instrueix als teus usuaris.
- Si cal canvia els passwords del correus afectats.
- Assegura que tens l'antivirus actualitzat i instal·lat a tots els equips.
- Si et demanen diners, no paguis. Primer consulta quines estratègies de desencriptació i/o desinfecció podem seguir.

Alerta: Virus/Malware Emotet

Aquests últims dies s'han incrementat els atacs del malware Emotet, dissenyat el 2014 amb l'objectiu de registrar dades personals i robar dades financeres. Aquest virus s'escampa i infecta mitjançant correus d'aparença normal, que sovint passen els filtres informàtics i no són detectats per la majoria de programes antivirus.

El remitent que figura en el correu, aparentment és o està relacionat amb una direcció de confiança o coneguda. Tanmateix, una vegada obert el correu la direcció és una altra i si s'obre el document adjunt, que apareix buit, es dona entrada al programa maliciós. El virus també pot segrestar llocs web i injectar-scripts maliciosos que descarreguen i instal·len Emotet a l'ordinador.

Els correus electrònics d'Emotet poden contenir imatges de marques conegudes dissenyades perquè semblin un correu electrònic legítim. S'intenta persuadir els usuaris perquè facin clic als arxius maliciosos utilitzant un llenguatge temptador sobre "La seva factura", "Informació de pagament" o possiblement un proper enviament d'empreses de missatgeria molt conegudes.

Es tracte de spoofing, és a dir, d'una suplantació de la identitat en què un atacant es fa passar per una entitat diferent a través de la falsificació de les dades, generalment amb usos maliciosos o d'investigació.

Els efectes immediats és l'enviament massiu de correus als destinataris existents a la bústia de sortida.

Emotet està més enfocat a infectar organitzacions governamentals, corporacions i pimes, però els usuaris particulars també estan en risc.

Primer de tot: prevenció

- Formació continua als usuaris
- Comproveu sempre qui és el remitent del correu electrònic.

  Si el correu electrònic suposadament prové d'un banc, verifiqui amb el seu banc si el missatge rebut és legítim. Si és d'un contacte personal, confirma si et van enviar el missatge. No confiar únicament en la confiança en virtut de la relació, ja que el teu amic o familiar també pot ser víctima d'spammers.
- Torneu a verificar el contingut del missatge.

  Hi ha errors de fet obvis o discrepàncies que es poden detectar: un avís d'un banc o un amic que han rebut alguna cosa de vostè? Revisar les carpetes d'elements enviats o de correu brossa. Mireu el text del correu si correspon a correus antics pel tema o la data. Canvi en l'idioma habitual del remitent: sol escriure en català i el missatge ve amb l'assumpte en castellà o en anglès... Aquests missatges de correu brossa també poden usar altres esquers d'enginyeria social per persuadir els usuaris que obrin el missatge.

  Cal vigilar els assumptes dels nostres correus electrònics, ja que els creadors de Emotet han recuperat una funcionalitat molt sofisticada de phishing llançada a l'abril de 2019, que consisteix a segrestar vells fils de correu electrònic i referències a l'usuari pel seu nom. D'aquesta manera tracten d'atreure els usuaris perquè obrin documents o enllaços perillosos.
- Abstenir-se de fer clic als enllaços al correu electrònic.

  En general, s'ha d'evitar fer clic als enllaços del correu electrònic. És més segur visitar qualsevol lloc esmentat al correu electrònic directament. Si ha de fer clic en un enllaç al correu electrònic, assegureu-vos que el vostre navegador utilitza la reputació web per verificar l'enllaç.
- Assegureu-vos de que els programes i usuaris de l'ordinador usin el nivell més baix de privilegis necessaris per completar una tasca.
- Posar totes les actualitzacions dels sistemes operatius dels equips i dels servidors.
- Protegir les dades amb les eines adequades. Anti-virus actualitzat i de pagament, Tallafocs i Polítiques d'accés pels usuaris.
- Sistema de Backup eficient i monitoritzat. Còpies al Núvol.

  Còpia de seguretat de dades importants. Una pràctica informàtica segura és garantir que tingui còpies de seguretat dels seus arxius. Recomanable el principi 3-2-1: tres còpies, dos mitjans diferents, una ubicació separada (servei d'emmagatzematge a núvol).
- Actualitzar els equips i adaptar-los als requeriments reals de l'empresa.
- No estalviar en allò que ens permet treballar més eficientment i amb seguretat.

Contacte ara amb nosaltres i t'ajudarem
93 883 68 99 - suport@btic.cat