Deloitte.

Upplýsingaöryggi

Vírinn

2. tbl. 3. árgangur, 31. janúar 2013

Fréttir um upplýsingatækni frá Áhættuþjónustu Deloitte ehf.

Áhættuþjónusta (ERS) er sérfræðihópur innan endurskoðunarsviðs Deloitte ehf. sem sérhæfir sig í innra eftirliti upplýsingakerfa, upplýsingaöryggi og endurskoðun upplýsingakerfa. Vírinn er gefinn út á tveggja vikna fresti og ætlaður m.a. stjórnendum, kerfisstjórum og almennum notendum upplýsingakerfa. Nýjustu fréttir Vírsins birtast jafnóðum á heimasíðu Deloitte á síðu **upplýsingaöryggisdeildar**.

Ný óværa sem herjar á Skype

Útskýrir aukinn fjöldi notenda Skype aukningu á óværu?

Fréttir eru farnar að berast af því að nýir vírusar séu farnir að herja á Skype spjallforritið. Að þessu sinni er um að ræða Shylock, vírus sem kom fyrst fram 2011 en hefur nú fengið yfirhalningu og kemur aftur enn skæðari en áður. Eldri útgáfur af Shylock voru helst tengdar við tilraunir til að stela bankaupplýsingum. Þetta nýja afbrigði stelur skrám úr tölvum, sendir og eyðir skilaboðum og sendir vinabeiðnir á fólk, og dreifir sér þannig á milli notenda. Smitleiðir eru hefbundnar, tölvupóstur og „snerting“ við sýkta miðla. Hugsanlega er þetta ekkert sem ekki hefur sést áður, en hér gæti verið komin fram vísbending um að vírusframleiðendur fari að leggja meiri áherslu á Skype nú þegar Microsoft hefur tilkynnt að þeir muni hætta að styðja MSN og benda öllum notendum á Skype. Hugsanlega er Shylock bara byrjunin.

Meira

Enn eitt botnetið fellt

Botnet sem eltist við bankaupplýsingar sýnir hversu einföld botnet* geta verið

Hollenska fyrirtækið Fox-IT hefur nýlega greint frá því að þeim hafi tekið að ráða niðurlögum Pobelka botnetsins, en Pobelka er rússneska og þýðir að hvítþvo. Þetta tiltekna botnet var helst að herja á viðskiptavini banka í Þýskalandi og Hollandi, og dreifði þá til þess Citadel og SpyEye óværunni, sem einhverjir lesendur Vírsins ættu að kannast við. Þessar óværur eru farnar að flytja fjármuni nokkuð sjálfvirkt á milli reikninga og komast framhjá sterkum vörnum. Var þetta botnet þá einungis að sækjast eftir bankaupplýsingum, frekar en að vera að daðra við margt eins og mörg

önnur botnet. Gróðinn var svo meðal annars notaður til að greiða fyrir þjónustu sem beindi fleiri tölvum og notendum í átt að botnetinu. Þykir Pobelka botnetið gott dæmi um hversu auðvelt getur verið að setja upp og hafa stjórn á botneti.

*Botnet er þegar sýktum tölvum er smalað saman og stjórnað af einum eða fáeinum aðilum, oftast í slæmum tilgangi.

Meira

Nýr veikleiki í Java kemur fram

Endalausar óværur hrekja framleiðendur og notendur frá Java

Það telst varla lengur til frétta þegar nýr veikleiki finnst í Java, en einn slíkur var einmitt að finnast nýlega. Þessi veikleiki er talinn komast framhjá helstu öryggisathugunum sem Java hefur. Oracle sem gefur út Java hefur áður brugðist við slíkum veikleikum með því að gefa út sérstakan („out-of-band“) plástur til að bregðast við veikleikum, en enn sem komið er hefur helsta lausnin verið að gera Java óvirkt í tölvunni, og kveikja ekki á nema nauðsyn krefji. Ýmsar vefsíður og vefsíðhlutar þurfa Java til að keyra, en fleiri og fleiri virðast vera að færa sig frá notkun Java, til dæmis yfir í HTML5 eða Flash, sem virðast vera öruggari leiðir til að hanna vefsíður.

Meira

Barracuda búnaður seldur með bakdyrum

Netvarnarbúnaður seldur með innbyggðum veikleikum

Komið hefur í ljós að búnaður sem hannaður er af Barracuda fyritækinu, til dæmis eldveggir, ruslvarnir og VPN búnaður, hefur innbyggðar bakdyr sem mögulegt er að misnota ef þekkingin er til staðar. Hönnunin átti að vera á þá leið að einungis væri hægt að nýta þessar bakdyr frá ákveðnum stöðum innan Barracuda fyrirtæksins, en komið hefur í ljós að svo var alls ekki, og að bakdyrnar voru aðgengilegar talsvert fleirum. Bakdyrnar virðast hafa verið til staðar frá 2003, og gerðu mögulegt að komast í grunnstillingar án þess að þurfa lykilorð. Barracuda hefur brugðist við að nokkru leyti, en samkvæmt sérfræðingum er þó ekki búið að loka fyllilega fyrir veikleikann. Okkur er ekki kunnugt um hvort Barracuda búnaður sé mikið notaður hér á landi.

Meira

Viðtakendur eru hvattir til að áframsenda Vírinn á áhugasama

Nánari upplýsinga um þjónustuframboð Deloitte á sviði upplýsingakerfa og upplýsingaöryggis veita:

Jón Kristinn Ragnarsson, sérfræðingur

Úlfar Andri Jónasson, kerfisfræðingur, MCTS, MCP

---

innlend lög, reglugerðir, viðskiptavenju og aðra þætti, og getur veitt sérfræðiþjónustu á starfssvæði sínu í gegnum dótturfélög, tengd félög, og/eða önnur félög.

Deloitte veitir bæði opinberum aðilum og einkafyrirtækjum í fjölmörgum atvinnugreinum endurskoðunar-, skatta-, ráðgjafar- og fjármálaþjónustu. Alþjóðlegt sérfræðinet Deloitte tengir saman sérfræðinga í 150 löndum þannig að saman fari ítarleg staðbundin þekking og alþjóðleg hæfni, viðskiptavinum til hagsbóta. Hjá Deloitte starfa um 200.000 sérfræðingar sem stefna saman að því að veita ávallt framúrskarandi þjónustu.