Iknedēļas ziņas
Sagatavotas 06.12.2016.
Numurs 2016/41

Zaudē 20000 EUR, apmaksājot izmainītus rēķinus

Kārtējie divi Latvijas uzņēmumi zaudējuši vairāk kā 20000 EUR katrs, apmaksājot rēķinus, kuros nomainīti saņēmēja bankas rekvizīti. Tāpat naudu zaudējis kāda Latvijas uzņēmuma ārzemju klients, kas veicis apmaksu par piegādājamo preci uz krāpnieku izveidotu kontu.
Lai iegūtu kontroli pār uzņēmuma e-pastu, uzbrucēji tā darbiniekiem nosūta ziņojumus, kas satur datorvīrusu, vai tā lejupielādes saiti. E-pasti tiek kvalitatīvi noformēti kā sūtījumi no potenciālajiem klientiem, kurjerpasta vai sadarbības partneriem.
Ar datorvīrusa palīdzību uzbrucēji iegūst pilnu kontroli pār upuru datoru un izmanto iegūtos e-pasta piekļuves datus, lai pārbaudītu uzņēmuma saraksti un pareizajā brīdī tajā ievietotu rēķinus ar izmainītiem apmaksas rekvizītiem.
Lai nekļūtu par šādas krāpšanas upuriem, nepieciešams izmantot kvalitatīvu un atjauninātu antivīrusu programmatūru, kā arī veikt papildu pārbaudes, sazinoties ar darījumu partneriem telefoniski gadījumos, kad rēķinā parādās citi bankas konti.

DDoS uzbrukums uzņēmumam

Pret kāda uzņēmuma datortīklu no 20. līdz 21. novembrim tika veikts apjomīgs DDoS uzbrukums, kurš tika ierobežots, atslēdzot interneta pakalpojumu sniedzēja tīklu no ārzemju interneta. Uzbrukuma organizatori sazinājušies ar uzņēmuma vadību un izteikuši vēlmi iegūt kontroli pār uzņēmuma daļām. Uzņēmums atteicās ar viņiem komunicēt, taču atkārtoti DDoS uzbrukumi uzņēmumam nesekoja.

Izspiedēja uzbrukums mājas lapai

Kādas mājas lapas uzturētāji savā Facebook kontā saņēmuši vēstuli, kurā pieprasīti 400 USD, par kuru nesamaksāšanu draudēts dzēst viņu mājas lapu. Uzbrucējs, nesaņemot prasīto summu, lapu tiešām izdzēsis.
Lapa tika atjaunota no rezerves kopijām un uzlabota to uzturošā servera drošība. Dati par šo izspiešanas mēģinājumu nodoti policijai.

Viltots e-veikals izkrāpj samaksu par preci

Kāds lietotājs, atsaucoties uz Facebook pamanītu reklāmu, samaksājis vairāk kā 100 EUR viltotā e-veikalā.
Veikals no kredītkartes noņēmis ne tikai summu par nepiegādāto preci, bet arī vairāk kā 15 EUR dažādas papildu „komisijas" maksas. Šobrīd krāpnieciskā vietne ir slēgta. Apkrāptajam pircējam CERT.LV ieteica sazināties ar savas kredītkartes izdevējbanku, lai risinātu naudas atgūšanas jautājumus.

Šifrējošo datorvīrusu izplata XLS failos

Vairāki datorlietotāji sūdzējušies CERT.LV par nezināmu personu sūtītiem e-pastiem ar pielikumu .XLS formātā.
Vēstules paraugs:

From: creditcontrol@maryli[redacted] [mailto:creditcontrol@mary[redacted]
Sent: Tuesday, November 29, 2016 10:41 AM
To:[redacted]
Subject: Please find attached a XLS Invoice 954163

Please find attached your Invoice for Goods/Services recently delivered. If you have any questions, then pleasedo not hesitate in contacting us.Karen Lightfoot -Credit Controller, Ansell Lighting, Unit 6B, Stonecross Industrial Park, Yew Tree Way, WA3 3JD. Tel: +44 (0)7375 235 512 Fax: +44 (0)7375 235 512

Pielikumā esošais fails satur Microsoft Office Macro komandas, kas veic Locky tipa vīrusa lejupielādi un upura datu šifrēšanu. Šifrētajiem failiem tiek pievienots paplašinājums .zzzz