

Iknedēļas ziņas
Sagatavotas 16.11.2016.
Numurs 2016/40

Izplata datorvīrusu ar tematu par nesamaksātu parādu

Kibernoziedznieki masveidā izsūtīja vēstules latviešu valodā par it kā nesamaksātu parādu. Pielikumos esošie faili saturēja datorvīrusu, kas paredzēts informācijas zagšanai un finanšu transakciju pārtveršanai no inficētā datora.

From Accounting <y-ogawa@daiko> >☆
Subject **Parada piedzinas pretenzija par Ligumu** 2016.11.09. 23:27
Reply to Accounting <noreply@> ☆
To ☆

Labdien, 10.11.2016. balstoties uz noslegto Ligumu nr.45 Jusu uzņēmumam tika sniegti pakalpojumi par kopejo summu 4262,00 eiro. Attiecīgi noslegta Liguma 3.punktam, pasūtītājs apņemas apmaksat pakalpojumus piecu darba dienu laikā no pakalpojuma izpildes dienas un attiecīgi 3.2. punktam, gadījuma ja pakalpojumi netiks apmaksāti noradītāja laikā, sākot ar sesto darba dienu tiks aprekināta kavejuma nauda 3.4% no pakalpojumu summas par katru nokavēto dienu. Līdz šim brīdim rekurs par sniegtajiem pakalpojumiem nav apmaksāts. Nemot vērā augstākminēto, lūdzam Jus, apmaksat parādu pilna apmēra līdz 14.11.2016. Gadījuma ja noteiktajā termiņā apmaksā tiks veikta tālāk vai vispār netiks veikta, mēs esam spiesti vērsties LR tiesā ar prasību par piespiedu parādu piedzinu.

1 attachment: Ligums_kopija_12199.zip 3,2 KB Save

Uzbrucēju sagatavotais kods tika izplatīts .zip arhīva pielikumos ar .wsf (Windows Script File) instrukcijām. CERT.LV iesaka ierobežot šādu failu piegādes, atvēršanas un izpildīšanas iespējas datorā.

Vairāk par WSH atslēgšanu: <https://cert.lv/lv/2016/04/pieejama-video-pamaciba-ka-atslegt-wsh>

Tīmekļa vietnes uzbrūk apmeklētāju ierīcēm

Ar jaunu sparū tiek izplatīts tā saucamais FakejQuery trojāns, kas pazīstams jau vairākus gadus. Šoreiz uzbrucēji ir identificējuši arī vairākas .lv domēnu zonā esošas ievainojamas vietnes, kas uzturētas uz novecojušas satur vadības sistēmas (Joomla, Wordpress, Drupal) versijas un izmantojuši tās kā platformu uzbrukumiem. Inficētās vietnes ir apzinātas un CERT.LV koordinē incidentu risināšanu.

Papildu informācija: <https://blog.sucuri.net/2015/11/jquery-min-php-malware-affects-thousands-of-websites.html>

Vilto e-pastus uzņēmuma vadītāja vārdā

CERT.LV saņēma vairākus ziņojumus par krāpšanas mēģinājumiem, kuros no uzņēmumiem mēģināts izkrāpt naudu ar uzņēmuma vadītāja vārdā sūtītu viltotu e-pastu. Krāpnieki pirms tam veikuši rūpīgu uzņēmumu mājas lapu izpēti, lai noskaidrotu uzņēmuma struktūru, uzņēmuma vadītāju, vadītāja e-pastu un uzņēmuma grāmatvedi, kuram adresēt viltoto sūtījumu.

Krāpniecisko e-pastu paraugs:

From: [redacted] [redacted]
Sent: Tuesday, November 8, 2016 11:56 AM
To: [redacted]
Subject: Maksājuma pieprasījums

Sveiki,

Man ir nepieciešams, lai jūs veiktu maksājuma pārskaitīšanu saņēmējam jau šodien. Vai esat pieejams, un kādi bankas dati jums ir nepieciešami, lai veiktu maksājumu?

Paldies

[redacted]

Lai attaisnotu kļūdaini sagatavoto tekstu, krāpnieki aizbildinās ar bojātu klaviatūru.

CERT.LV aicina būt uzmanīgiem un rūpīgi izvērtēt saņemtos e-pastus pirms tiek veiktas jebkādas finansiālas darbības. Ja e-pasti ir neprofesionāli sagatavoti, tajos ir steidzamības vai slepenības aspekts, drošāk ir veikt telefona zvanu un pārliecināties, vai šāds e-pasts tiešām ir sūtīts.