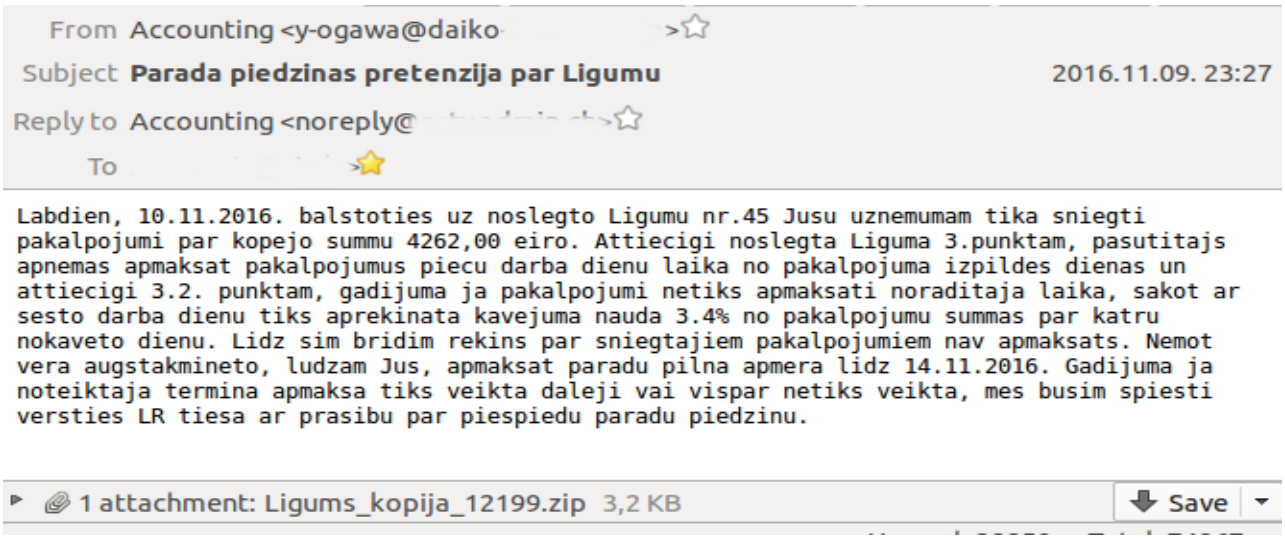
Iknedēļas ziņas
Sagatavotas 16.11.2016.
Numurs 2016/40

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.



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

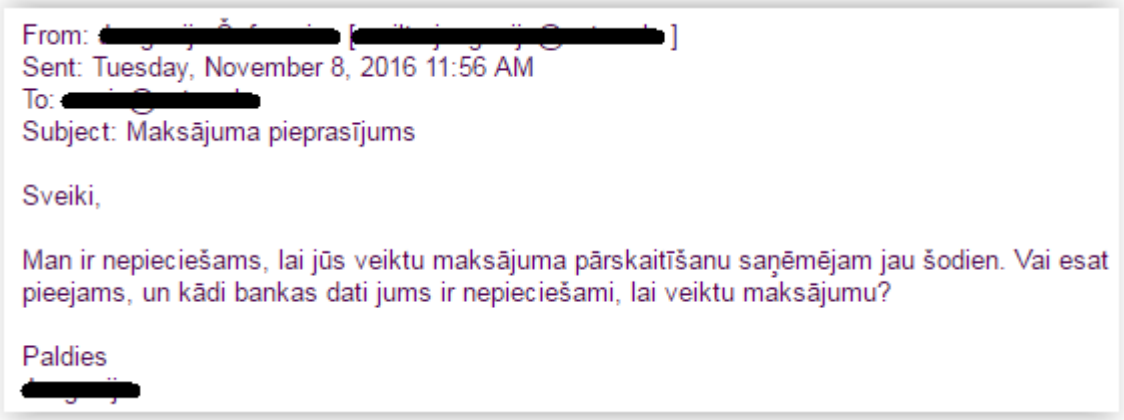
Tīmekļa vietnes uzbrūk apmeklētāju ierīcēm

Ar jaunu sparu 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.