Iknedēļas ziņas
Sagatavotas 26.02.2016.
Numurs 2016/8

Kontakti: prese@cert.lv
Tālrunis: 67085888

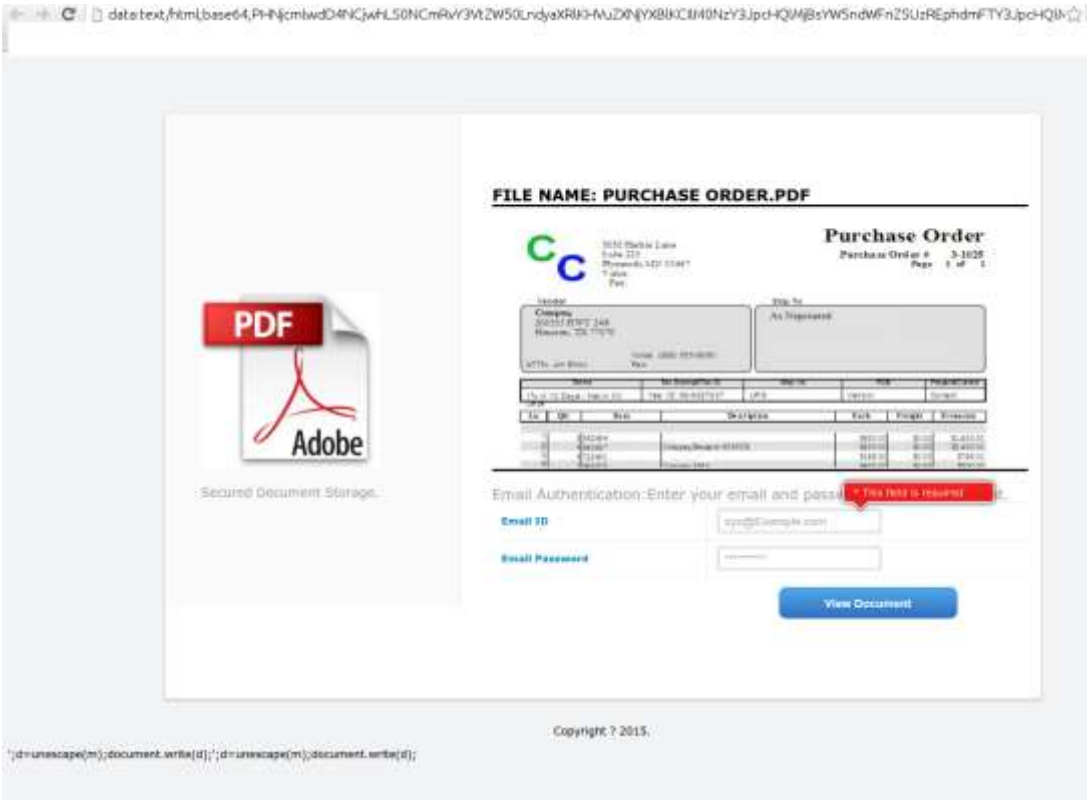
Mobilais telefons patvaļīgi izsūta SMS

Kāda lietotāja mobilais telefons bez tā ziņas ir izsūtījis apmēram 200 SMS ziņojumus ar tekstu "Let's video chat and text on imo! get the free app http://ww24.getvideocalls.com"
Apmeklējot norādīto saiti, tā pārvirza apmeklētāju uz legālajā Google Play piedāvāto aplikāciju ImoIM, pievienojot atsauci uz iepriekšējo lapu, www.24.getvideocalls.com.
ImoIM aplikācija nav kaitīga, bet šādas reklamēšanas metodes var radīt zaudējumus tālruņa īpašniekam.
Turpinās pārbaude, lai konstatētu, kura no tālrunī uzstādītajām aplikācijām ir izsūtījusi šīs SMS.

Izsūta viltus rēķinus, lai izkrāptu e-pasta paroles

Krāpnieku izsūtītos viltus e-pastos tika ievietots aicinājums apskatīt atsūtīto rēķinu, kas ved uz saīsināto saiti. Caur šo saiti lietotājs tiek pāradresēts uz speciālu lapu, kas paredzēta e-pasta piekļuves datu izkrāpšanai. Lapas īpašnieki uz aicinājumiem to slēgt nav atsaukušies.

Lapas ekrānšāviņš:



Uzlauztās vietnēs turpina izplatīt vīrusus

Divās interneta lapās tika ievietoti Angler EK Eksploit Kit komponenti. Tas nozīmē, ka apmeklējot šādu lapu Internet Explorer pārlūkā, lapas kodā tiek pievienoti kaitīgi elementi, kas mēģina veikt datorvīrusu lejupielādi un izpildi apmeklētāju datorā. Apmeklētājiem, kas neizmanto Internet Explorer, kaitīgais kods netiek padots. Abas lapas izmanto populārās CMS - Joomla un Wordpress. Pēc brīdinājuma lapas tika salabotas vai slēgtas.

Šifrētājvīrusa vietā izplata "banku vīrusu"

Kampaņa, kuras ietvaros pagājušajās nedēļās tika izplatīti MS Office dokumenti ar kaitīgu makro kodu, kas lejupielādē Locky šifrētājvīrusu, šobrīd atgriezusies pie Dridex banku trojāņa izplatīšanas.
Latvijā ir konstatēti vairāki Locky sašifrēti datori.