

Iknedēļas ziņas  
Sagatavotas 04.03.2016.  
Numurs 2016/9

Kontakti: [prese@cert.lv](mailto:prese@cert.lv)  
Tālrunis: 67085888

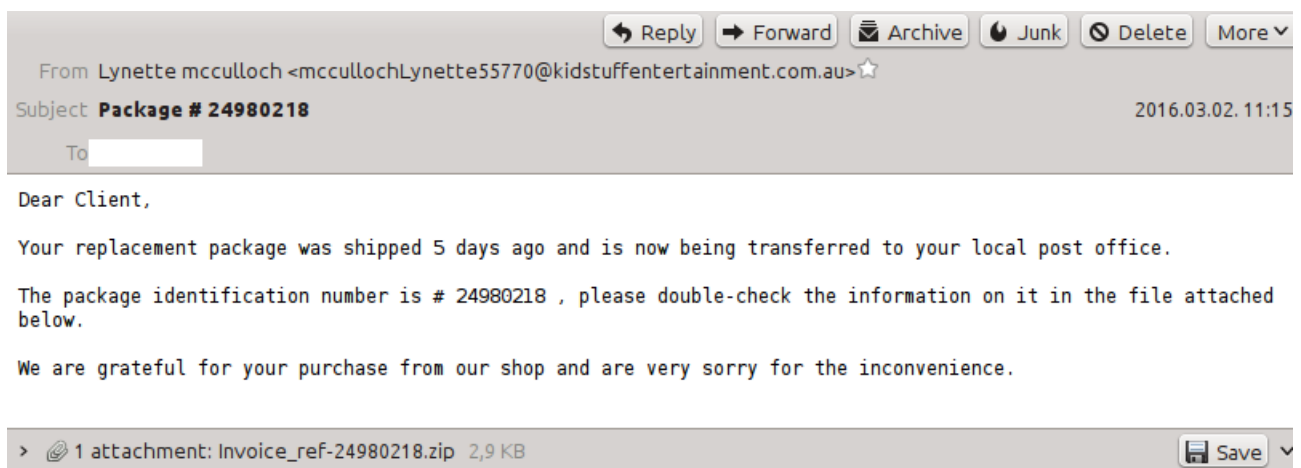
## ***Jauna ievainojamība DROWN apdraud drošu datu pārraidi***

Atklāta jauna ievainojamība DROWN (CVE-2016-0800), kas apdraud drošus TLS datu pārraides savienojumus. Apdraudēti ir serveri, kas atbalsta novecojušu SSLv2 šifrēšanu un kuros nav atjaunināts OpenSSL. Lai nepakļautu sevi DROWN riskam, iesakam neizmantot SSLv2 šifrēšanu un serveros atslēgt šo funkciju.

Vairāk par šo ievainojamību lasiet: <https://www.openssl.org/news/secadv/20160301.txt>

Latvijas IP adresu apgabalā esošās ievainojamās iekārtas ir apzinātas, un to uzturētāji brīdināti.

## ***Viltus paziņojumos par pasta sūtījumiem izplata šifrētāJVīrusu Locky***



The screenshot shows an email client interface. At the top, there are buttons for 'Reply', 'Forward', 'Archive', 'Junk', 'Delete', and 'More'. The email header includes 'From: Lynette mcculloch <mccullochLynette55770@kidstuffentertainment.com.au>', 'Subject: Package # 24980218', and the date '2016.03.02. 11:15'. The 'To' field is redacted. The main body of the email contains the following text:

Dear Client,

Your replacement package was shipped 5 days ago and is now being transferred to your local post office.

The package identification number is # 24980218 , please double-check the information on it in the file attached below.

We are grateful for your purchase from our shop and are very sorry for the inconvenience.

At the bottom, there is a notification for an attachment: '1 attachment: Invoice\_ref-24980218.zip 2,9 KB' with a 'Save' button.

Masveidā izsūtīti viltus e-pasta paziņojumi par piegādātiem pasta sūtījumiem. Paziņojumiem pievienots ZIP formāta arhīvs, kas satur Javaskript failu. Atverot pievienoto failu ar interneta pārlūku, tas veic nejašu nosaukuma .exe faila lejupielādi uz lietotāja %TEMP% direktoriju. Lejupielādētais fails satur LOCKY šifrējošo vīrusu.

## ***Krāpnieki izspiež naudu, draudot publicēt privātas fotogrāfijas***

Kāds sociālā tīkla *V Kontakte* (vk.com) lietotājs tajā saņēmis draudu vēstuli, ka tiks publicētas privātas fotogrāfijas, ja netiks samaksāta izpirkuma maksa. Izpirkums ticis samaksāt, bet bilžu publiskošanu tas nav kavējis, papildus pieprasot vēl naudu, lai to pārtrauktu.

CERT.LV atgādina - nekad nemaksājiet šādiem izspiedējiem! Un rūpīgi izvērtējiet, kādas fotogrāfijas publicēt internetā.

## Izķēmota Augstākās tiesas mājaslapa



Ar SQL injekcijas tipa uzbrukumu neilgu brīdi tika izķēmota Latvijas Republikas Augstākās tiesas mājaslapa. Ievainojamie komponenti ir atrasti un salaboti.

### ***Nekorekta personas datu pārraide***

Kāda komunālo pakalpojumu sniedzēja tīmekļa vietnē fizisko personu dati tiek vākti, neizmantojot drošu SSL/TLS savienojumu, tādējādi radot iespēju tos pārtvert tīkla datu plūsmā. Šāda rīcība neatbilst labajai praksei, kā vācami un apstrādājami fizisko personu dati (<http://www.dvi.gov.lv/lv/datu-aizsardziba/organizacijam/8-labas-prakses-principi-fizisko-personu-datu-apstrade/>). Lapas īpašnieks brīdināts.