Iknedēļas ziņas
No 24.08. līdz 28.08.2015.
Numurs 2015/05

Kontakti: prese@cert.lv
Tālrunis: 67085888

Kompromitēts serveris izsūta masveida mēstules FBI vārdā, ar mērķi izkrāpt privātpersonu datus un naudas līdzekļus

Kompromitēto tīmekļa serveri uzbrucēji izmanto kā mēstuļu izsūtīšanas resursu un starpniekserveri pēdu slēpšanai. CERT.LV informē servera īpašnieku par kaitnieciskajām aktivitātēm un sniedz instrukcijas situācijas risināšanai.
CERT.LV rīcībā nav informācijas, ka šīs uzbrukumu kampaņas rezultātā Latvijā būtu kāds upuris.

Krāpnieciskās vēstules teksts:

ANTI-TERRORIST AND MONETARY CRIMES DIVISION
FBI HEADQUARTERS IN WASHINGTON, DC
FEDERAL BUREAU OF INVESTIGATION
J. EDGAR HOOVER BUILDING
IA 935 Pennsylvania Avenue, NW
WASHINGTON, DC 20535-0001

This is to officially inform you That It Has Come to our notice and we thoroughly Have completed an investigation with the help of our network monitoring system intelligence That your e-mail address email That was Among the award won lottery Which you did not claim, we want to let you know That one of the bank worker Where arrange your fund was deposited With His friend to eat as the owner of the e-mail That Which They won the prize claim your fund, but now your fund has-been recovered from them and the People that claim your fund has-been arrested. If You receive any e-mail that you 'did not Understand That is from unknown person to you please do forward it to us to verify and bring the person to justice.

We Have Gone Through Your identification record and verified We Have a lot of things about you. It Has Come to the attention of our money trafficking investigation department, that you 'have some funds valued 800,000.00 Pounds on your name, the payment is awaiting adjudication Said We Have esta winning authorized to be paid to you, esta are from lottery funds.

RE-CONFIRM, NAMES, ADDRESS, PHONE NUMBER, AGE / SEX, OCCUPATION AND COUNTRY, TO AVOID DOUBLE YOUR CLAIM OF FUND.

Your immediate response is needed
JAMES B. COMEY
FBI DIRECTOR

Uzlauztā neuzticīgu partneru vietne ashleymadison.com saturēja vairāk kā 2000 Latvijas interneta lietotāju kontu informāciju

Pēc globālā kiberuzbrukuma vietnei *ashleymadison.com* hakeri tiešsaistē publicējuši vairāk nekā viena miljona lietotāju personas datus.
Arī Latvijas interneta lietotājus arvien biežāk masveidā skar globālas uzbrukumu kampaņas tādu sociālo tīklu lietotāju kontiem kā Twitter.com, Facebook.com, Google, utt. Tādas pašas tendences ir arī ar tiešsaistes maksājumu sistēmām Paypal, interneta veikaliem/izsolēm ebay.com, amazon.com un iekārtu ražotājkontiem Apple.
Latvijas interneta lietotāju, kuri kļūst par globālu kiberuzbrukumu kampaņu mērķi, dati ir daudz grūtāk pasargājami, ja atrodas ārvalstīs uzturētās vietnēs.

Vairākas kompromitētas tīmekļa vietnes Latvijā piedalās pikšķerēšanas uzbrukumā ar mērķi izkrāpt datus no American Express klientiem

Tīmekļa vietnēm uzbrukumi realizēti pagaidām nenoskaidrotā veidā, iegūstot FTP kontu paroles. Uzbrucēji ir spējuši pieslēgties tīmekļa vietnes administratora FTP kontam un augšupielādēt savu kaitīgo saturu. CERT.LV atgādina, ka drošu paroļu izvēle un atbilstoša glabāšana ir vienlīdz svarīga visiem Jūsu tiešsaistes kontiem.
Vairāk informācijas par drošu paroļu izvēli meklējiet CERT.LV uzturētā portālā www.esidross.lv.

Latvijas uzņēmuma noliktavas vadības sistēmas tika inficētas ar failu šifrēšanas vīrusu, kas paralizēja uzņēmuma darbību

Uzņēmums veica inficēto iekārtu pārinstalēšanu no rezerves kopijām, kas diemžēl liedza CERT.LV veikt pilnvērtīgu incidenta analīzi. Uzbrucējiem netika maksāts par failu atšifrēšanu, **jo uzņēmumam bija pieejamas noliktavas uzskaites sistēmas rezerves kopijas.**