Iknedēļas ziņas
No 10.08. līdz 14.08.2015.
Numurs 2015/03

Kontakti: prese@cert.lv
Tālrunis: 67085888

Kāds interneta ziņu portāls piedzīvo un sekmīgi atvaira hakeru uzbrukumu

Kāda ziņu portāla sistēmu administratori sazinājās ar CERT.LV un sniedza informāciju par notikušu kiberuzbrukumu viņu interneta vietnei.
Veicot incidenta analīzi noskaidrots, ka uzbrukums veikts no kādas Latvijas IP adreses, pielietojot automatizētus ievainojamību meklēšanas rīkus. Uzbrucējs meklējis iespējas veikt SQL injekcijas, lai veiktu nesankcionētas manipulācijas ar datu bāzi. Informācija par kaitnieciskajām darbībām tika nodota interneta pakalpojumu sniedzējam, gala lietotājs ir brīdināts.

Notikuši vairāki DDoS uzbrukumi tīmekļa vietnēm Latvijā. Uzbrukumus saista viena pazīme, uzbrucējs visdrīzāk ir viens un tas pats

Vairāku tīmekļa vietņu turētāji ir vērsušies pie CERT.LV, informējot par DDoS incidentiem. Iegūstot detalizētāku tehnisko informāciju, noskaidrots, ka tiek pielietots HTTP DDoS un visus gadījumus vieno pazīme - “undefined” URI laukā.

Piemērs: `GET www.cert.lv/lv/undefined`

Šādu uzbrukumu ir salīdzinoši vienkārši atvairīt. Uzbrukumā iesaistītas arī IP adreses no Latvijas. CERT.LV ir sniedzis norādījumus cietušajiem uzbrukuma ietekmes mazināšanai un sazinājies ar pakalpojumu sniedzējiem, informējot par kaitnieciskajām darbībām un avotiem. Ir noskaidrots, ka uzbrukumā piedalās inficētas iekārtas, pārsvarā kompromitēti koplietošanas tīmekļa serveri.

Uzlauztas 8 tīmekļa vietnes un iesaistītas pikšķerēšanas uzbrukumos pret Brazīlijas bankām un Paypal maksājumu sistēmu

Kompromitētās vietnes tika uzturētas uz novecojušas satura vadības sistēmas Joomla 1.5. versijas.
Šobrīd Joomla satura vadības sistēmai jau ir pieejama 2.5.28 versija, taču joprojām ir simtiem tīmekļa vietņu, kas neatjauno programmatūru un tādējādi ir nedrošas. Nedrošās vietnes šobrīd ir padarītas nepieejamas, līdz to uzturētāji veiks nepieciešamos drošības uzlabošanas darbus.