

Diena.lv

Db.lv

Aizkraukle

Alūksne

Bauska

Gulbene

Jelgava

Liepāja

Valka

Abonēšana

Visas ziņas

Meklējam sirdsmāsiņu

Dienas Starts

Horoskopi

TV programma

Dienas projekti

Sludinājumi

E-avīze

Sestdiena

Ienākt ar Diena ID


Otrdiena
31. jūlijsVārda diena
Ruta, Rūta, Sijaīta, AnželikaLaika ziņas
+18°C, DR vējš, 2
m/s
[Latvijā](#) [Pasaulē](#) [Sports](#) [KDiena](#) [Business](#) [Tehnoloģijas](#) [Izklaide](#) [Tautas policija](#) [Diena TV](#) [Foto](#) [Londona 2012](#)
[Ziņas](#) [Kriminālvēstis](#) [Politika](#) [Rīgā](#) [Novados](#) [Viedokļi](#)


Foto: Kristians Putniņš, Dienas mediji

Kāda Latvijas ministrija piedzīvojusi mērķtiecīgu hakeru uzbrukumu ⁹

LETA. 2012. gada 30. jūlijs 14:36

Kāda Latvijas ministrijai uzbrukuši hakeri, apstiprināja informācijas tehnoloģiju (IT) drošības incidentu novēršanas institūcijā CERT.LV.

Netiek atklāts, kurai ministrijai uzbrukts, bet publiskota informācija par hakeru izmantotajiem rīkiem un iespējamiem mērķiem. Uzbrukuma laiks netiek konkretizēts - var nojaust, ka tas noticis pirmajā pusgadā.

Izmantots īpaši viltīgs mērķēts uzbrukums ar nolūku zagt informāciju vēl nezināma uzbrukuma autora vajadzībām. Uzbrukuma rīks veidots, lai informācijas nopludināšana notiktu ministriju datoru lietotāju parastās interneta lietošanas laikā, šifrētā veidā, lietotājam nezīnot, kas notiek. Datorus, kurus inficēja uzbrukumā lietotā ļaundabīgā programmatūra, bija iespējams vadīt no kāda servera Lielbritānijā, taču tas nenozīmē, ka uzbrukuma veicējiem bija kāds sakars ar šo valsti, skaidroja CERT.LV.

"Konkrētajam uzbrukumam tika izmantoti domēna vārdi, kas reģistrēti dažas dienas pirms veikta uzbrukuma. Kontrolcentram tika izmantots tieši šai kampaņai paredzēts serveris, kas tika Trērs vienā no Lielbritānijas datu centriem. Fakts, ka daļa uzbrukumā iesaistīto resursu tika uzturēta Lielbritānijā, neveido nekādu saistību politiskā līmenī. Arī Latvijas datu centru resursus uzbrucēji nereti izmanto nelikumīgām darbībām un uzbrukumiem pret IT sistēmām citās valstīs, jo internetā nav tādu robežu kā fiziskā telpā," norādīja datu drošības iestāde.

Latvijas gadījumā uzbrukums tika realizēts, upurim izsūtīt speciāli sagatavotu e-pastu, kura pielikumā bija Microsoft Word dokuments. Upurim atverot dokumentu, fonā tiek izpildītas uzbrucēja programmatūras dotās instrukcijas, uzstādītas ļaundabīgās programmatūras komponentes un veidota saziņa starp upura datoru un uzbrucēju kontrolcentru.

Saistītie raksti

Skārletas Johansones kaifoto nopludinātājam jāmaksā prāva soda nauda **6**

ASV apsūdz Latvijas pilsoni par neatļautu piekļuvi brokeru kontiem **1**

Hakeri izdzēsuši portāla kompromat.lv arhīvu **11**

Hakeri Zviedrijā zog datus, bet Latvijā izķēmo lapas

Jauni kiberdraudi. Kaitīgi QR Kodi, surrogātpasts Skype un troješi viedtālruniņiem

Izkēmotas 27 Latvijas un ar Latviju saistītas mājaslapas

Kibernoziedznieki uzbrukuši 12 Latvijas mājaslapām, tostarp krišnaītiem un maziem uzņēmumiem

Dienas dziesma



DIENAS DZIESMA:
lesaka Ketija
Dombrovska

Dienas rīts



Raidījums Dienas Rīts ēterā atgriezīsies 6.augustā **2**

Diena jautā

Vai ātro kredītu aizdevēju darbība būtu jāierobežo stingrāk? **0**

- Jā
- Nē
- Jāiztiek no tā, ko nopelna
- Kredītēšana jāatļauj tikai bankām

Balsot

Parādīt atbildes

[Citi jautājumi](#)

"Uzbrucējam šajā stadijā ir pilna kontrole pār upura datoru, par ko lietotājam nav ne jausmas. Uzbrukums tiek realizēts, izmantojot kādu no ievainojamībām dokumentu apstrādes programmā," teikts eksperta sagatavotajā paziņojumā.

Mērķētus uzbrukumus datu drošības aprindās uzskata par īpaši bīstamiem, jo tos veic konkrētu upuru izspiegošanas vai darbības traucēšanas nolūkos. Savukārt parastas ļaundabīgas programmatūras izplatītāji cenšas inficēt iespējami plašu IT resursu loku, un tiem ir vienalga, kam pieder "nozombētie" datori, jo tos izmanto vērienīgai surogātpasta sūtīšanai, dažādām krāpšanām, piekļuves bloķēšanas uzbrukumiem u.tml.

Pie mērķētiem uzbrukumiem pieskaita arī pirmā "kiberieroča" *Stuxnet* parādīšanos, kas izstrādāts, lai traucētu specializētas industriālu iekārtu vadības sistēmas, visticamāk, lai sabotētu Irānas urāna bagātināšanas centrifūgas. *Stuxnet* izstrādāja kādas valsts vai valstu slepenie dienesti, uzskata datu drošības kompānijas *Kaspersky Lab* un citi eksperti.

Kā informē *CERT.LV*, Latvijas gadījumā izmantots datoru uzlaušanas rīks *Enfal*, kas iepriekš fiksēts uzbrukumos pret valsts iestādēm un citiem mērķiem dažādās pasaules valstīs. *Enfal* sākotnēji saistīja ar KĶĶ, bet tas pamanīts arī uzbrukumos pret IT resursiem šajā valstī.

Datu drošības iestāde uzsver, ka pēc *CERT.LV* pieprasījuma Latvijas incidentā iesaistītie resursi tika atslēgti, bet ministrijas IT administratori saņēma nepieciešamās instrukcijas. Šajā gadījumā gan paši ministrijas administratori bija savlaicīgi parūpējušies par programmatūras drošības ielāpu uzstādīšanu, lai infekcija nespētu izplatīties.

Par mērķēto uzbrukumu tika vēstīts *CERT.LV* pārskatā par darbību šī gada otrajā ceturksnī, taču bez sīkāka apraksta par notikušo.

Jau ziņots, ka otrajā ceturksnī *CERT.LV* ir reģistrējis un apstrādājis 1274 augstas prioritātes incidentus un reģistrējis 43 489 zemas prioritātes incidentus.

CERT.LV darbojas kopš 2011.gada 1.februāra un ir atbildīga par informācijas tehnoloģiju drošības veicināšanu Latvijā.

iesaki rakstu draugiem

Pievieno komentāru

Lasīt visus 9 komentārus

2403 EUR, Pļavnieki

120517 EUR, Carnikava

225000 EUR, Dubulti

590000 EUR, Saulkrastu l.t.

1630 EUR, Āgenskalns

520 LVL, Centrs

Ziņas

Ierosināta Vitronic Baltica un partneri tiesiskās aizsardzības lieta

Arhitekts par Gaismas pili: lecerētais kalna gals atgādina gaiļa seksti **29**

Skolās ieviests finanšu mācību **13**

Mūžībā aizgājis 8.Saeimas deputāts Uldis Mārtiņš Klauss

Lembergs gatavo vēl vienu sūdzību ECT - par politisko vajāšanu **30**

Varētu kļūt zināms, kurš izstrādās jauno sabiedriskā medija koncepciju

Mikroautobusu reforma Rīgā pagaidām iestrēgusi **1**

Galerija

Šodien laikrakstā Diena



[Iepriekšējos numuros](#)

[Abonēt](#)



Kā es jutos kad... GIF'os.
[2]

Dienas žurnālos