Foto: Kristians Putniņš, Dienas mediji

Kāda Latvijas ministrija piedzīvojusi mērķtiecīgu hakeru uzbrukumu 9

LETA. 2012. gada 30. jūlijs 14:36

Kādai 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 laika, šifrētā veidā, lietotājam nezinot, 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 veiktā uzbrukuma. Kontrolcentram tika izmantots tieši šai kampaņai paredzēts serveris, kas tika īrēts 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 izsūtot 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 kailfoto 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, surogātpasts Skype un trojieši viedtālruņiem

Izķēmotas 27 Latvijas un ar Latviju saistītas mājaslapas

Kibernoziedznieki uzbrukuši 12 Latvijas mājaslapām, tostarp krišnaītiem un maziem uzņēmumiem

"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 Ķīnu, 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.

Galerija