Diena. - 13.03.2024

Visaugstāko apdraudējumu Latvijas kiberfrontē rada Krievijas vadītās kibergrupas

Кіберугруповання на чолі з росією представляють найбільшу загрозу на кіберфронті Латвії

Згідно зі звітом про діяльність Служби державної безпеки Латвії (VDD) за 2023 р. найбільшу загрозу на латвійському кіберфронті представляють кіберугруповання, очолювані російськими спецслужбами, однак китайські кіберпідрозділи також почали виявляти помітний інтерес до Латвії. На ситуацію у сфері кібербезпеки продовжувала впливати триваюча війна в Україні, яку росія також поширила в кіберпростір. Кібератаки були здійснені не лише проти України, а й проти країн-членів НАТО та ЄС, які підтримують Україну, зокрема Латвії.

https://www.diena.lv/raksts/latvija/zinas/visaugstako-apdraudejumu-latvijas-kiberfronte-rada-krievijas-vaditas-kibergrupas-14314616

Visaugstāko apdraudējumu Latvijas kiberfrontē rada Krievijas specdienestu vadītās kibergrupas, tomēr arī Ķīnas kibervienības ir sākušas izrādīt manāmu interesi par Latviju, teikts Valsts drošības dienesta (VDD) pagājušā gada darbības pārskatā.

Lielākos kiberspiegošanas draudus Latvijai joprojām rada naidīgu ārvalstu specdienestu kontrolē esošas kibergrupas. Tieši šīm kibervienībām ir visaugstākā sagatavotība, resursi un iemaņas, lai plānotu un realizētu sarežģītas kiberizlūkošanas operācijas.

Ārvalstu specdienestu vadīto kibergrupu mērķi ir dažādi. Visbiežāk tie kompromitē datorsistēmas, proti, neatļauti iefiltrējas šajās sistēmās, lai tūlītēji izgūtu sensitīvu izlūkinformāciju, sabotētu datorsistēmu darbību vai arī iznīcinātu tajās esošos datus. Tomēr ļoti bieži naidīgo valstu kontrolētie grupējumi veic datorsistēmu kompromitēšanu, lai iegūtu un nostiprinātu ilgstošu slēptu klātbūtni šajās sistēmās, teikts pārskatā.

Šādu slēptu pastāvīgu klātbūtni specdienestu vadītās kibergrupas var izmantot ilgtermiņā, lai nepieciešamības gadījumā veiktu jebkuru no iepriekš uzskaitītajām ļaundabīgajām darbībām upura datorsistēmā.

Tāpat Krievijas specdienestu kontrolē esošās kibergrupas pērn turpināja īstenot tā dēvētos piegādes ķēdes uzbrukumus, kas patlaban ir uzskatāmi par vienu no bīstamākajiem un grūtāk identificējamiem kiberdrošības apdraudējumiem. Tie ir komplicēti uzbrukumi, kuri

parasti tiek īstenoti, lai iefiltrētos un veiktu kaitnieciskas darbības vai nu lielā daudzumā datorsistēmu vienlaikus, vai konkrētās labi aizsargātās sistēmās.

Šādos gadījumos kibernoziedznieki potenciālajam mērķim uzbrūk caur kādu no tā piegādes ķēdes dalībniekiem. Piemēram, pirms piegādes potenciālajam mērķim ar ļaunatūru var tikt inficētas datorsistēmas, programmatūra vai tās atjauninājumi.

VDD vērtējumā liela daļa kiberuzbrukumu joprojām izdodas informācijas tehnoloģiju pārvaldītāju un lietotāju pieļautu kļūdu dēļ. Kiberuzbrucēji savā labā izmanto neprasmīgi konfigurētus datortīklus un vāju kiberhigiēnas ievērošanu.

VDD vērsis uzmanību, ka augstus kiberspiegošanas riskus rada vāji aizsargātiem lietotāju kontiem piešķirtas nesamērīgas piekļuves tiesības, piemēram, valsts nozīmes datubāzēm.

Kopumā secināts, ka kiberapdraudējuma līmenis Latvijas kibertelpā aizvadītajā gadā saglabājās nemainīgi augsts, tomēr situācija kopumā bija un arī pašlaik ir vērtējama kā stabila. Situāciju kiberdrošības jomā turpināja ietekmēt Ukrainā notiekošais karš, ko Krievija izvērsa arī kibertelpā. Kiberuzbrukumi tika īstenoti ne tikai pret Ukrainu, bet arī kara skarto valsti atbalstošām NATO un ES dalībvalstīm, tajā skaitā Latviju.

Kopš Krievijas iebrukuma Ukrainā Latvijas valsts institūcijas un citi stratēģiski svarīgi objekti ir būtiski uzlabojuši gatavību un aizsardzības spējas pret kiberuzbrukumiem, tādējādi stiprinot Latvijas kibertelpas drošību. Pateicoties veiktajiem sagatavošanās pasākumiem, lielākā daļa valsts iestāžu un citu haktīvistu izraudzīto mērķu pērn spēja tūlītēji reaģēt, izmantojot jaunākos aizsardzības risinājums.

Saistībā ar minēto lielākā daļa Krievijas haktīvistu uzbrukumu bija neveiksmīgi, nenesot uzbrucējiem gaidītos rezultātus