Iknedēļas ziņas
Sagatavotas 08.07.2016.
Numurs 2016/25

Kontakti: prese@cert.lv
Tālrunis: 67085888

Brīva piekļuve valsts iestādes datubāzei

Kādā valsts iestādes mājas lapā tika atklāta konfigurācijas kļūda, kas autorizētiem lietotājiem ļāva piekļūt citu personu datiem, kas atrodas iestādes datubāzē. Līdzīga situācija savulaik bija Valsts ieņēmumu dienestā un izraisīja VID datu noplūdes skandālu. Šobrīd nav zināms, vai pieejamā informācija tikusi ļaunprātīgi izmantota, bet atbildīgās personas kļūdu operatīvi izlaboja.

Maršrutētāju skenēšana

Kāda valsts iestāde saskārusies ar MikroTik maršrutētāju skenēšanu. Izmantojot MikroTik maršrutētāju konfigurācijas lietotni Winbox, notika mēģinājumi veikt nesankcionētus pieslēgumus ar maršrutētājos pēc noklusējuma iestatītajiem piekļuves datiem. Ja ražotāja uzstādījumi nav mainīti, uzbrucējs var piekļūt maršrutētājam un izmantot to ļaunprātīgām darbībām. Drošības palielināšanai būtu ieteicams ne tikai nomainīt ražotāja uzstādījumus, bet arī aizliegt piekļuvi pie administrācijas paneļa no publiskā tīkla un definēt IP adreses, no kurām šo piekļuvi atļaut.

TP-Link zaudējusi kontroli pār konfigurācijas domēna vārdiem

TP-Link ir viens no pasaulē lielākajiem Wi-Fi maršrutētāju ražotājiem, kura produktos izmantotie domēna vārdi tplinklogin[.]net un tplinkextender[.]net šobrīd ir pieejami iegādei. Lai gan pats uzņēmums apgalvo, ka visi produkti, kas iegādāti un izmanto šos domēna vārdus, tiks automātiski novirzīti uz iekšējo iestatīšanas lapu, un tas neradīs nekādus drošības apdraudējumus, tomēr drošības eksperti uzskata, ka šie domēna vārdi, nonākot uzbrucēju rokās, viegli varētu tikt izmantoti uzbrukumos miljoniem maršrutētāju. Vairāk: https://threatpost.com/top-router-maker-tp-link-loses-control-over-configuration-domain/119072/

Atklāta jauna Mac ļaunatūra – Eleonora

Atklāta jauna, uz Mac OS X mērķēta ļaunatūra. Ļaunatūra iestrādāta viltotā failu konvertēšanas lietotnē EasyDoc Converter, kas tiek piedāvāta populārās Mac lietotņu un programmatūru vietnēs. Lietotne neveic paredzētās failu konvertēšanas funkcijas, bet izpilda ļaunprātīga skripta lejupielādi. Šī ļaunatūra spējīga piekļūt failu sistēmai, attālināti veikt ļaunprātīga koda izpildi, kā arī piekļūt tīmekļa kamerai. Pirms veikt jebkādas lietotnes lejupielādi savā ierīcē, ieteicams pārbaudīt tās izcelsmi, veiktos atjauninājumus un atsauksmes no citiem lietotājiem.
Vairāk: https://blog.malwarebytes.com/cybercrime/2016/07/new-mac-backdoor-malware-eleanor/