Iknedēļas ziņas
Sagatavotas 15.03.2017.
Numurs 2017/7

MikroTik iekārtu lietotājiem jāveic atjauninājumi

07.03.2017. Wikileaks publicēja dokumentu kopu, kas satur informāciju par dažādiem ASV Centrālās izlūkošanas pārvaldes (CIP) ielaušanās rīkiem. Viens no dokumentiem saturēja rīka "ChimayRed" aprakstu, kas ļauj attālināti iegūt piekļuvi MikroTik maršrutētājiem, ja tajos aktivizēts iebūvētais HTTP serveris, un tas nav aizsargāts ar ugunsmūri.
MikroTik ir novērsuši ievainojamību RouterOS versijās v6.38.5 un 6.39rc49
CERT.LV iesaka lietotājiem veikt MikroTik iekārtu programmnodrošinājuma atjaunināšanu.
Ja atjaunināšana nav iespējama - nepieciešams ugunsmūrī atļaut piekļuvi HTTP serverim tikai no noteiktām IP adresēm, vai atslēgt šo funkciju.

Vairāk par CIP informācijas noplūdi: http://thehackernews.com/2017/03/wikileaks-cia-hacking-tool.html

Ievainojamība pakļauj riskam vairākas mājas lapas

Martā CERT.LV saņēma informāciju, ka kādā populārā satura vadības sistēmā atrasta ievainojamība. Ievainojamība ļauj veikt neautorizētu piekļuvi mājaslapas datubāzei, un iegūt paroles, kuras šī vadības sistēma šifrēja nedrošā veidā. Ievainojamības tips – SQL injekcija.
Ietekmētas bijušas apmēram desmit mājas lapas, to starpā vairākas pašvaldību pārraudzībā esošas mājas lapas.
CERT.LV sazinājās ar lapu uzturētājiem un informēja par atklāto ievainojamību. Lapu uzturētāji ir uzsākuši lapu labošanas darbus.

Atrasta ļaunatūra 38 ražotāju Android iekārtās

Check Point Software pētnieki atklāja nopietnu infekciju 38 dažādu ražotāju Android iekārtās. Tika noskaidrots, ka ļaunatūra telefonos tikusi uzinstalēta telefonu piegādes, nevis ražošanas procesā. Iekārtās tika veikta ļaunatūras izpēte un atklāti divi ļaunatūru paveidi - Loki and SLocker.
Loki ir trojāns, kas darbojas pašā Android operētājsistēmas kodolā un iegūst "root" tiesības. Trojāns spēj piekļūt aplikāciju sarakstam, pārlūka vēsturei, kontaktu sarakstiem, zvanu vēsturei un atrašanās vietas datiem.
SLocker, savukārt ir mobilais izspiedējvīruss.

Vairāk par Android iekārtu ļaunatūru: http://thehackernews.com/2017/03/android-malware-apps.html

Piezīme: Rakstā minēts, ka viena no iespējām, kā noņemt ļaunatūru, ir veikt "root" tiesību iegūšanu, taču CERT.LV atgādina, ka "root" tiesību iegūšana salauž iebūvēto ierīces aizsardzību un pakļauj to infekciju riskam nākotnē.

Pieejami padomi drošākai interneta lietošanai

Interneta lietotājiem pieejami bezmaksas informatīvi materiāli par drošību interneta vidē. Materiāli veidoti kiberdrošības iniciatīvas APSTĀJIES. PADOMĀ. PIESLĒDZIES. (STOP. THINK. CONNECT.) ietvaros. Kiberdrošības iniciatīvai CERT.LV pievienojās 2016. gadā.
CERT.LV vietnē www.esidross.lv pieejami dažādi ar drošību saistīti ieteikumi - kā veikt pavasara tīrīšanu datorā, kā izvēlēties drošus wifi tīklus, un kā sarunāties ar tīņiem par drošību.

Materiāli pieejami angļu valodā.
Vairāk: https://www.esidross.lv/2017/03/10/apstajies-padoma-piesledzies/

Uzdodas par Google Chrome pārlūku

Parādījusies jauna kaitnieciska aplikācija, kas uzdodas par Goolge Chrome pārlūku, lai izvilinātu no lietotājiem kredītkaršu datus.
Eksperti ir secinājuši, ka aplikācijas dizains ir izveidots ļoti ticami, tāpēc lietotājiem ir jāizvērtē programmu lejupielāžu avoti.
Šobrīd konkrētā aplikācija izplatīta Nīderlandē, bet ir tikai laika jautājums, kad tā var tikt pārtulkota arī citās valodās.
Vairāk: https://www.bleepingcomputer.com/news/security/credit-card-stealer-disguises-as-google-chrome-browser/