Iknedēļas ziņas
Sagatavotas 05.09.2016.
Numurs 2016/33

Apple datorus inficē populārā torentu programma Transmission

Apple lietotāji jau otro reizi šajā gadā tiek pakļauti riskam inficēt savus datorus, uzstādot populāro torentu lejuplādes programmu Transmission. Šīs programmatūras izstrādātāju oficiālā vietne tika uzlauzta šī gada martā un uzbrucēji, modificējot oriģinālo programmu, izplatīja tās inficēto versiju, kas bija parakstīta ar neoriģinālu, taču derīgu izstrādātāja sertifikātu.
Kļuvis zināms, ka 28.08.2016. uzbrukums tika sekmīgi realizēts atkārtoti un ikviens, kas lejuplādēja Transmission programmatūru laika posmā no 28. - 29.08.2016. saņēma tās inficēto versiju v2.92. Izplatītās infekcijas nosaukums ir OSX/Keydnap, kurai ir tuva radniecība ar šogad jau izplatīto OSX/KeRanger, tāpat abas ir paredzētas autentifikācijas rīku zagšanai, kā arī, lai nodrošinātu uzbrucējam kontroli pār inficēto datoru.

Kāpēc šis incidents bija iespējams?
Oficiālā izstrādātāja tīmekļa vietne tika uzlauzta un noteiktu laiku viss tās saturs bija hakeru kontrolē, ieskaitot lietotāju lejuplādei paredzēto Transmission programmatūru. Pēc incidenta oficiālā Transmission versija tiek piedāvāta lejuplādei no Github.com.
Lai arī Apple kompānija ir ieviesusi aizsardzības mehānismus, kontrolējot programmatūras uzticamību ar kriptogrāfiskiem parakstiem, šajā gadījumā inficētā Transmission versija bija parakstīta ar cita, leģitīma izstrādātāja parakstu, līdz ar to Apple to uzskatīja par derīgu uzstādīšanai.

Kā noskaidrot, vai dators ir inficēts?
Lietotājiem jāmeklē šādi kaitīgie faili:

- /Applications/Transmission.app/Contents/Resources/License.rtf
- /Volumes/Transmission/Transmission.app/Contents/Resources/License.rtf
- $HOME/Library/Application Support/com.apple.iCloud.sync.daemon/icloudsyncd
- $HOME/Library/Application Support/com.apple.iCloud.sync.daemon/process.id
- $HOME/Library/LaunchAgents/com.apple.iCloud.sync.daemon.plist
- /Library/Application Support/com.apple.iCloud.sync.daemon/
- $HOME/Library/LaunchAgents/com.geticloud.icloud.photo.plist

Kaitnieciskas Android aplikācijas inficē pusmiljonu viedierīču

Arī Android oficiālā programmatūras vietnē kārtējo reizi nonākusi ļaunatūra, kas nosaukta par DressCode, tāpēc, ka galvenokārt tika izplatīta spēļu aplikācijās, kas saistītas ar virtuālu pucēšanos.
Pilns inficēto aplikāciju saraksts atrodams pētījuma autoru mājas lapā:
http://blog.checkpoint.com/2016/08/31/dresscode-android-malware-discovered-on-google-play/

DressCode inficētās iekārtas tika padarītas par robotu tīkla sastāvdaļu un uzbrucēji tās spēja kontrolēt attālināti. Pagaidām pastāv uzskats, ka uzbrucēju mērķis ir bijis nelikumīga finansiāla labuma gūšana, manipulējot ar reklāmu saturu.

Latvijā aktīvās ļaunatūras kampaņas

Šajā periodā aktīvi izplatītas tika tādas kampaņas kā šifrējošais vīruss Locky, JAVA attālinātās vadības ļaunatūra Adwind un paroļu atjaunošanas rīka LaZagne pielietošana uzbrukumiem.

Ja pirmās divas uzbrukumu kampaņas ir vērojamas jau ilgāku laiku, tad pēdējā, kurā uzbrucēji izmanto leģitīmu paroļu atjaunošanas rīku LaZagne, ir kas mazliet atšķirīgāks.
Visās pieminētajās uzbrukumu kampaņās ļaunatūras piegādes veids ir līdzīgs – e-pasts ar pielikumu, kurā ir .zip, .jar, .wsf, .pdf fails, kuru lietotājām atverot tiek piegādāts kaitīgais kods. Visbiežāk pats pielikuma fails paredzēts tikai patiesā vīrusa lejuplādei un izpildīšanai uz upura datora.
Arī šajā kampaņā LaZagne rīks tiek izplatīts ļaunprātīgos nolūkos caur e-pastiem ar .jar pielikumiem. E-pasti bija noformēti angļu valodā un izsūtīti, izmantojot ar banku maksājumu uzdevumiem saistītu tematiku.
Ja lietotājs pielikuma .jar failu izpilda, tiek lejuplādēts LaZagne rīks no domēna www.videosdelmatematico[.]com