21. мај 2019.

ПРИКУПЉАЊЕ ДИГИТАЛНИХ ДОКАЗА

Увод

Напади у сајбер простору су свакодневна појава, како у Републици Србији, тако и у свету. У току једног дана се деси велики број покушаја упада у информационе системе, рачунаре или мобилне уређаје. Занимљива је чињеница да су све чешће мете напада и конзоле за игру, дигиталне камере, навигациони системи или Интернетом повезане ствари (енг. *IoT*), као и уређаји за бежични приступ Интернету (енг. *Wi-Fi*). Циљеви ових напада могу бити различити, од крађе личних података корисника, злоупотреба налога на друштвеним мрежама, остваривање терористичких циљева, па све до шпијунаже. Позадина свих ових напада најчешће буде стицање противправне финсансијске користи за нападача.

Прикупљање дигиталних доказа

Када корисници информационих система предузимају превентивне мере за заштиту од сајбер напада, препоручене од стране Националног ЦЕРТ-а, већи део наведених типова напада може бити спречен. Међутим, одређени број напада се ипак успешно реализује и корисницима буде нанета штета. Поставља се питање, шта корисници могу да предузму у таквим ситуацијама, како би причињена штета била сведена на минимум и рачунар био поново спреман за рад.

Корисницима, који постану жртве успешног напада хакера, Национални ЦЕРТ Републике Србије препоручује предузмање следећих корака:

- прекинути конекцију рачунара са Интернетом, било да је реч о директној конекцији путем кабла, или *Wi-Fi* уређаја,
- уколико је рачунар део одређеног информационог система, неопходно је да корисници из рачунара извуку мрежни кабл, како не би инфицирали остале рачунаре у мрежи.

Веома је важно напоменути да се не сме прекидати довод напајања рачунара електричном енергијом, нити поновно покретати оперативни систем рачунара (енг. *Restart*). Тиме се онемогућава квалитетно прикупљање дигиталних доказа, односно спровођење форензичке анализе од стране Одељења за високотехнолошки криминал при Министарству унутрашњих послова Републике Србије (vtk@mup.gov.rs), као и Посебног тужилаштва за борбу против високотехнолошког криминала Републике Србије (http://www.beograd.vtk.jt.rs/).

За потребе очувања дигиталних доказа, неопходно је креирање идентичне копије хард-диска, која садржи целокупну структуру самог диска, као и све податке, програме, фајлове и фолдере који су били на рачунару у тренутку напада. Постоји неколико софтверских решења за креирање копије (нпр. Symantec Ghost, EaseUS Todo Backup) које корисници могу употребити.

Поред креирања копије хард-диска, корисници могу сачувати и друге податке који могу бити од велике користи приликом спровођења истражних радњи од стране надлежних органа, као што су:

- чување лог фајлова, који представљају забележен скуп података о активностима одређеног уређаја,
- заглавље имејл поруке (енг. *e-mail header*) – представља скуп метаподатака који могу садржати детаље о пошиљаоцу малициозне поруке,
- узнемиравање путем Интернета (енг. *cyberbullying*) корисници могу забележити снимком одређене текстуалне поруке, или видео записа који је постављен на друштвеним мрежама, а представља одређени вид узнемиравања корисника путем Интернета.

По завршеном креирању резервне копије и прикупљању наведених података, корисници могу почети са опорављањем рачунара, које укључује:

- поновно инсталирање оперативног система (нпр. *Windows, Linux, macOS*) које садржи све закрпе (енг. *patch*),
- поновно инсталирање последње доступне верзије апликативних решења која су била коришћена на инфицираном рачунару,
- поновно инсталирање и покретање последње доступне верзије антивирусног софтвера издате од стране произвођача.

Уколико има више инфицираних уређаја на мрежи, неопходно је за сваки од њих спровести све наведене кораке. Након опоравка је неопходно испратити рад инфицираних рачунара, како бисмо утврдили да нема неправилности у њиховом даљем раду.

Закључак

Свакога дана се на Интернету појави око 3000 нових малициозних садржаја и није реално очекивати да се корисници могу одбранити од сваког од њих, али применом превентивног приступа знатно можемо смањити вероватноћу успешности хакерских напада на рачунаре и остале електронске уређаје и тиме омогућити неометан рад информационих система и присуство на Интернету.