

Ukradeni oblaci i ostale ljetne razbibrige



Vrijeme je godišnjih odmora, sistemci odmaraju na plaži ili plijeve vrt na djedovini. Na odmor su ponijeli knjige koje su davno nabavili, ali nije bilo prilike da ih se pročita. Službeni mobiteli su na dohvat ruke, s notebooka se povremeno provjerava stanje servera i mreže na poslu. Neprijatelj nikad ne spava, zar ne? Usput se prate vijesti iz struke, a možda se stigne naučiti nešto novo. Ljeti se sve radi usporeno, treba puniti baterije, odmoriti se za nove izazove, ali radoznalost se ne može zatomiti. Otkrili smo zanimljive vijesti iz svijeta informacijske sigurnosti. Ali odmak od svakodnevnih briga tjera na razmišljanje, pa i traženje šireg konteksta iz kojeg se potpunije sagledava naša svakidašnjica.

Iz medija saznajemo da su napadači godinama provaljivali na servere mobilnih operatera, kako bi se domogli podataka o pozivima, odnosno o tome tko je koga zvao, u koje vrijeme i s koje lokacije. Umjesto napada na pametne uređaje odabranih korisnika koji su napadačima zanimljivi, odlučili su pronaći slabe točke operatorskih servera. S javnih servera dobili bi pristup internoj mreži i redom osvajali umrežene uređaje, tražeći akreditive, povećavajući ovlasti, nastojeći steći što potpuniji pristup. O tome nas je izvijestila tvrtka Cybereason koja se bavi zaštitom "endpoint" uređaja. Operaciju Soft Cell otkrili su prije godinu dana, ali izgleda da su napadi počeli još 2012., možda i ranije. Oprezni su kada govore o počiniteljima, kažu da sve ukazuje na kinesku grupu APT 10, ali ostavljaju otvorenom mogućnost da je taj trag podmetnut kako bi se prikrilo identitet pravog počinitelja. Više detalja pronaći ćete [ovdje](#) [1].

Što da se kaže na to? Znali smo da su ti podaci dostupni operaterima i preko njih vlastima ukoliko imaju valjan nalog, a možda i bez njega. Sad smo saznali da su se tih podataka dočepale i vlasti nekih drugih država, uz pomoć hakera u uniformi. Ima li još uopće smisla govoriti o privatnosti? Naravno da ima smisla, danas više nego ikad, jer je upravo danas najugroženija, a svima nam je važna.

Reutersovi istraživački novinari objavili su 26. lipnja opsežan članak o tome kako su napadači iz Kine najprije "osvojili" cloudove dviju renomiranih tvrtki, pazite sad, HP-a i IBM-a! Kad su u tome uspjeli, koristili su ih da bi s njih vršili napade na klijente ovih informatičkih divova. Popis je popriličan, na listi žrtava je i tvrtka Ericsson, izravan konkurent kineskim tvrtkama na tržištu telekomunikacija. Napadi su trajali godinama, od 2014. do 2017. Kad bi provala bila otkrivena, računala očišćena, napadači bi se vratili s novim oružjima i igra bi se ponavljala. Napadači su identificirani kao grupe hakera povezane s Kineskim Ministarstvom Državne sigurnosti (i tu se spominje APT 10). Ugrabili su mnoštvo povjerljivih informacija koje pripadaju tvrtkama i vladi SAD, s nakanom da se osnaže kineski ekonomski interesi. Štivo je zanimljivo, preporučujem da ga pročitate u cijelosti, a dostupno je na ovom [linku](#) [2].

Ransomware je maliciozni softver koji kriptira datoteke na korisničkim računalima, a korisnik dobije poruku da će dobiti šifru za dekripciju ako uplati nemalu sumu na anonimni bitcoin račun. Neki od kolega sistemaca imali su priliku поближе upoznati tu napast nakon što su njihovi korisnici neoprezno kliknuli na privitak dobijen uz phishing mail. Kako ova inačica kriminalne djelatnosti dobija na zamahu, pojavile su se tvrtke koje nude da će razbiti enkripciju bez plaćanja kriminalcima. Ako su podaci dragocjeni, a nemate valjan backup, lakše ćete se odlučiti da platite dobrim dečkima, nego kriminalcima, zar ne? No ProPublica, neprofitni medij koji istražuje zloupotrebe moći, otkriva način na koji bar neke od tih tvrtki posluju. Oni plate ucjenjivačima, a zatim otključaju korisničke podatke i naplate korisniku cijenu ucjene plus svoju zaradu. Podlo, zar ne? Američko ministarstvo Domovinske

sigurnosti tvrdi da se dnevno dogodi oko 4000 ransomware napada, tako da ovaj biznis cvjeta, a nepoštene tvrtke pomažu da i dalje bude uspješan. Izvješće je dostupno [ovdje](#) [3].

Za identifikaciju ljudi koriste se otisci prstiju (zaslugom Ivana Vučetića, koji je naše gore list), pa zatim novije tehnologije poput softvera za prepoznavanje lica, analize DNK, a sad se pojavljuje još jedna metoda. MIT Technology Review otkriva nam da svaki čovjek ima drugačije otkucaje srca. Američko Ministarstvo obrane naručilo je izradu tehnologije koja pomoću infracrvenog lasera na daljinama do 200 metara otkriva jedinstveni ritam bila i tako omogućuje identifikaciju. Ako se izradi bolji laser, bit će to moguće i s veće daljine. Čemu će to služiti? Otkrivanju terorista, koji su se prurušili da zavaraju softver za prepoznavanje lica? Prepoznavanju vlastitih vojnika na bojišnici, da se izbjegne prijateljska vatra? Ili će to koristiti atentatori kako bi pogodili pravu metu? Sve ovisi o tome tko će tu tehnologiju imati na raspolaganju i kakve su mu namjere.

Mogli bismo ovako nastaviti s prenošenjem (loših) vijesti do besvijesti. Ali vaš omiljeni sistemac čita i knjige koje je pripremio za godišnji odmor, koje nisu informatičke, prije spadaju pod "opću kulturu". Jedna od njih je iz Hararijeve trilogije koja je prevedena i kod nas (Sapiens, Homo Deus, 21 savjet za 21 stoljeće). Harari kaže da su u prošlosti čovječanstvo desetkovale tri pošasti: glad, bolest i ratovi. Razvojem civilizacije, znanosti i tehnologije danas su sve tri prijetnje praktički eliminirane. Hrane ima dovoljno za sve, lijekova također, a ratova je sve manje. Današnjem stanovniku razvijenog svijeta veću prijetnju predstavlja Coca Cola nego ratovi i terorizam, jer više ljudi umire od dijabetesa nego od nasilja (tipičan primjer Hararijeva smisla za humor, ali on takve tvrdnje podupire statističkim podacima). Svijet nije savršen, ali se neprestano kreće nabolje, a slijedeći korak bit će produžavanje života, potraga za besmrtnošću. Wow! Kakva pohvala znanosti i nepoljuljana vjera u Čovjeka!

Harari je načitan i znanstveno orijentiran mislilac koji nam nudi drugačiji pogled na povijest homo sapiensa. Druga knjiga koju sam čitao na plaži djelo je čovjeka koji nije imao priliku obrazovati se, ali je nekim čudom dobio iznenađujući uvid i razumijevanje svijeta. Zanimljivo je da se u nekim zaključcima ova dva različita autora slažu.

Martinus Thomsen je rođen u siromašnoj danskoj obitelji 1890. Radio je kao pastir, a zatim se zaposlio u mljekari. 1921. je doživio duhovno prosvjetljenje, a s njim je dobio "kozmički uvid" u razvoj života. U knjizi Sudbina čovječanstva konstatira stanje suvremenog svijeta: ima hrane za sve, a ljudi gladuju. Ima lijekova za sve, a ljudi umiru od bolesti. Ima dovoljno strojeva i konjskih snaga, a ljudi rade u znoju lica svog. Imamo sjajne škole i fakultete, znanost, crkve gdje propovijedaju ljubav prema bližnjem, a pokazujemo genijalnost u izmišljanju ubojitih oružja. Čovječanstvo bi trebalo proglasiti nemoralnim ili ludim! No to su samo razvojne faze, jer skupljamo iskustva, učimo i napredujemo. Evolucijski je čovjek u fazi razvoja inteligencije, ali je istovremeno još napola životinja koja ubija da bi preživjela. Razum nije posve razvijen, čovjekom upravljaju emocije koje nisu osviještene. Nacionalizam je sebičnost nacija, ali je istovremeno svijet toliko premrežen trgovinom, savezima i međunarodnim udruženjima (Internetom, dodali bismo), da narodi više nisu izolirane i neovisne države, već provincije u internacionalnom svjetskom carstvu. Ono je doduše još u zametku, nema svjetsku vladu i globalno važeće zakone koji bi štitili sve ljude podjednako, pa mu nedostaje pravda. U takvom svijetu najjači prigrabe vlast, a oni nisu najpravedniji ili najmoralniji, već često najsebičniji. Ljudi su za Martinusa "stanovnici" ovog planeta, grupirani u narode koji se naoružavaju, tako da jači mogu ugnjetavati i izrabljivati slabije stanovnike. To je stanje koje treba prevladati, razvojem inteligencije, znanosti, izgradnjom globalnog društva čiji je zametak UN (i EU). Takva zajednica više neće imati vanjskog neprijatelja, pa će nestati potreba za naoružavanjem! Svijetom bi tada konačno mogli upravljati najmudriji, a ne najsebičniji pojedinci.

Martinusove su knjige prevedene na brojne svjetske jezike (pa i hrvatski), ali je najpopularniji u Skandinaviji gdje ga smatraju filozofom i mistikom.

Čitajući loše vijesti koje prevladavaju u medijima, i one koje se odnose na informacijsku sigurnost kao i dnevno političke, čovjeka pomalo hvata depresija i defetizam. Što ja tu mogu, svojim malim snagama, doprinjeti? Zar Trumpov slogan "Amerika prije svega" ne podsjeća na Hitlerov "Deutschland uber alles" (sebičnost nacija)! Zar nam sada nije jasnije zašto nacionalistima svih boja EU predstavlja trn u oku? Zar nam nije jasnije zašto su u Vladu dospjeli ljudi koji obavljaju javnu funkciju za svoju osobnu korist (sebičnost političara)?

Čitajući na plaži Hararija i Martinusa možemo se opustiti, nasmejati, zabaviti, ali i razumjeti da nije sve tako crno, da svijet ide na nabolje, čovječanstvo evoluira. Još je pred nama mnogo posla, ali svatko od nas može doprinjeti time što će pošteno obavljati svoj posao, zar ne? Angažirati se u nekoj dobrotvornoj akciji, paziti kome dajemo glas na izborima, razotkrivati loše stvari i jasno se i glasno opredijeliti protiv njih, umjesto da samo sliježemo ramenima. Svaki se mali korak zbraja.

Dok sam na plaži surfao i tražio informacije za ovaj članak, notebook mi je uz glasni Puf! prestao raditi. Nije mu prijalo globalno zatopljavanje, a ni naša domaća bura. Znao kako to ide, ako nešto treba poći po zlu, poći će po zlu u najgori mogući trenutak. Kako ću održati rok i objaviti članak na vrijeme, u malom mistu na poluotoku, bez igdje ikog poznatog? Situacija se brzo i lako razriješila, pišem na posuđenom računalu. Nema toga što malo ljudske solidarnosti ne može riješiti.

sub, 2019-07-13 20:51 - Aco Dmitrović **Kategorije:** [Kolumna](#) [4]

Vote: 0

No votes yet

story_tag: [informacijska sigurnost](#) [5]

Source URL: <https://sysportal.carnet.hr/node/1852>

Links

- [1] <https://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/>
- [2] <https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/>
- [3] <https://www.propublica.org/article/sting-catches-another-ransomware-firm-red-mosquito-negotiating-with-hackers>
- [4] <https://sysportal.carnet.hr/taxonomy/term/71>
- [5] <https://sysportal.carnet.hr/taxonomy/term/101>