Preklapanje svjetova

Sezona odmora jenjava, već se radi punom parom. Sistemac se vratio s godišnjeg i odmah su ga dočekali problemi. Ovog puta je to novi *ransomware*, nazvan Zepto. Radi se o novoj verziji notornog Lockyja, koja je prošla kroz obranu na perimetru i dospjela u *Inbox* užurbanog korisnika, kojeg je dočekao nagomilan posao. Kliknuo je na privitak, ne razmišljajući. Zepto mu je kriptirao sve dokumente kojih se dočepao, u My Documents, na Desktopu. Pozadinu radne površine zamijenio je svojom stranicom u kojoj korisnika obavještava da mora platiti ucjenu, kako bi dobio alat za dekriptiranje i svoj privatni ključ. Cijena prava sitnica, 4 bitcoina!

Treba li reći da korisnik nema backup svojih datoteka? Treba li reći da nije odmah isčupao mrežni kabel iz svog računala? Googlao je, naravno sa zaraženog računala, našao uzaludne upute za uklanjanje virusa u kojima piše da to ne radite sami, pa ih je ispisao na mrežnom pisaču. Radi se o multifunkcionalnom uređaju, kopirki/skeneru/printeru. Sprava je podešena tako da se korisnici autenticiraju, a onda im ispiše dokument, a u slučaju skeniranja, skenirani dokument pošalje kao PDF u share na njihovom računalu. Korisnici koji su tog jutra skenirali dokumente začudili su se kad su u shareu našli čudna imena datoteka sa .zepto ekstenzijom.

Tada se na sceni pojavljuje sistemac. Sluša korisnika, postavlja pitanja. Gasi zaraženo računalo i sve mrežne printere. Nakon ponovnog uključivanja printera, Zepto više ne kriptira korisničke shareove. Korisnikovo računalo zapljenjuje i nosi ga u lab. To jest na svoj radni stol, niste valjda mislili da mu je ustanova dala prostoriju za lab? Zašto bi lab uopće bio potreban? Zato jer ima izdvojenu mrežu, pa ne ugrožava ni korisnike ni servere. Iz skladišta sistemac korisniku donosi novo računalo, da može raditi. Zaraženo računalo boota sa rescue CD-a proizvođača antivirusnog softvera. Antivirus ne otkriva ništa. Pokušava s CD-om drugog, pa trećeg proizvođača, opet ništa.

Sistemac zatim boota *live Linux* distribuciju, priključuje USB tvrdi disk na kojeg snima bitcopy cijelog diska zaraženog računala. Zatim koristi softver za spašavanje datoteka s oštećenih medija, *photorec*. *Photorec* izvlači na tisuće datoteka, smješta ih u desetke direktorija. Prije nego iz tog mnoštva izdvoji Office dokumente, slike i PDF-ove, sistemac na brzinu instalira *clamav*, besplatni anitivirus, i pušta ga da pregleda spašene datoteke. Besplatni antivirus pronalazi *Trojan downloader* i nekakvog *worma*. Eto zašto je trebalo odmah iščupati mrežni kabel!

Sistemac se nada da je Zepto otvorio korisnikove datoteke, kriptirao ih, spremio kao nove datoteke, a stare samo pobrisao. U tom slučaju je pobrisan samo pokazivač na početak datoteke, pa bi photorec mogao rekonstruirati izbrisane dokumente. Ukoliko je virus pametan i napravio *wipe* originalnih dokumenata, ništa od spašavanja.

Photorec je iz slike diska izvukao na tisuće dokumenata. Neki su nečitljivi, na primjer imaju extenziju .doc ili .docx, ali ih Word ne otvara (otvara ih Libre Office :). Ako ih i uspije otvoriti, pokazuje gomilu "smeća". Da bi automatizirao proces, sistemac piše *one linere* koji sve datoteke s extenzijama .doc i docx prebacuje u jedan direktorij, xls-ove u drugi, pdf-ove u treći itd. Tada traži među njima uzorke kako bi u jednom potezu izbrisao sve dokumente koji zapravo nisu dokumenti. Još malo ručnog otvaranja dokumenata, eliminacija nekoliko datoteka koje su promakle skriptama za brisanje, pa sve snima na dva DVD-a i odnosi korisniku neka se sam zabavlja. Nakon nekoliko dana, korisnik u jednom dahu zahvaljuje za spašene dokumente, ali je istovremeno ljut jer mu nisu spašeni neki drugi, koji su mu još važniji. Što da mu sistemac odgovori na to? Spašeno je što se dalo spasiti. Obrisana datoteka postaje slobodan prostor na na disku koji OS koristi za nove podatke. Zato se ne može sve spasiti. Ali to korisnika ne zanima. Nedostaju mu neke važne datoteke, on bi probao

nagovoriti upravu da plati hakerima crnošeširašima za dekriptiranje.

Tu je tehnički dio rješavanja problema završio, počinju administrativne zavrlame. Da bi računovodstvo platilo ucjenu, najprije traže da im donesete tri ponude! Probajte vi dobiti službene ponude od kriminalaca, s nazivom tvrtke, adresom, OIB-om i pečatom! Osim toga, plaćanje dolazi u obzir samo u kunama, kuna je jedina službena valuta u Republici Hrvatskoj! Postoji procedura za plaćanje u stranim valutama, ali ne i za Bitcoine.

Na stranicama Porezne uprave našli smo ovakvo mišljenje:

"07. svibnja 2015. Porezna uprava donijela je mišljenje o naplati PDV-a na transakcije virtualnim valutama kao što je bitcoin. Kao što smo ranije pisali, HNB bitcoin ne smatra sredstvom plaćanja u Hrvatskoj (“… bitcoin ne predstavlja novac, niti sredstvo plaćanja u Republici Hrvatskoj niti stranu valutu odnosno strano sredstvo plaćanja”). HNB također navodi da “… stavovi europskih država u odnosu na status virtualnih valuta (bitcoin) međusobno razlikuju te da neke države bitcoin smatraju proizvodom, neke imovinom, a neke financijskim instrumentom.

U skladu s tim PU donijela je mišljenje da se bitcoin transakcije mogu osloboditi plaćanja PDV-a. No, PU je svjesna da je od švedskog Vrhovnog suda zatraženo očitovanje o poreznom tretmanu bitcoina te da će njihova odluka u konačnici imati utjecaja i na porezni tretman bitcoina u Republici Hrvatskoj."

Nakon prikupljanja ponuda plaćanje bi trebala odobriti uprava, odnosno osoba ovlaštena za odobravanje isplata. Sretno vam bilo u pokušaju obrazloženja ovog troška! Bitcoin trenutno vrijedi oko 620 $, za četiri bitcoina trebalo bi dati blizu 17.000 kn. Kako u ovoj besparici opravdati takav trošak? Nema novaca ni za znanstvenu literaturu, edukaciju, stručne skupove... Jedini izvediv način je, čini se, da sam korisnik kupi Bitcoine i plati ucjenu. Ali on za to neće ni čuti, neka to plati ustanova! Nisu to njegove privatni dokumenti!

Sistemac razmišlja sistemski, pa se pita kako preduhitriti buduće napade na korisničke podatke? Backup je rješenje. Korisnicima su podijeljeni USB stickovi, uvijek mogu dobiti DVD-ove za izradu kopija. Ali stickovi su nekim čudom nestali, nitko ih više ne može pronaći, a svi su zatrpani poslom u toj mjeri da jednostavno ne stignu kopirati dokumente na DVD-ove! Sistemsko rješenje bio bi program koji bi automatski radio kopije korisničkih podataka. Kad bi ustanova imala novaca za takve stvari! Obično se backup smatra nebitnim sve dok se ne dogodi ozbiljan gubitak podataka. U ovom slučaju, bilo bi potrebno da više od jednog korisnika izgubi podatke. Po mogućnosti ne obični korisnici, nego netko iz uprave. Sistemac zna slobodno, *open source* rješenje. Zove se Backuppc, mali pametni softver otvorenog koda koji čak ne traži instalaciju klijenata na korisnička računala. Radi tiho, u pozadini, spaja se korisniku na računalo, kad jednom napravi *full backup* dalje radi samo inkrementalne kopije. Toliko je diskretan da korisnici i ne osjete da im se kopiraju podaci. Uz to radi kompresiju i deduplikaciju podataka, tako da ne rasipa prostor na serveru.

Gle čuda, sistemac je na svom računalu nedavno, kao da je znao, podigao virtualku na kojoj je Backuppc već instaliran i konfiguriran, spreman za korištenje. Trebalo bi samo dokupiti disk(ove) za podatke. O tome je htio pregovarati s upravom nakon godišnjeg, a Zepto je zapravo dobro došao, sad će se lakše odobriti kupovina dodatnog diskovlja. Jupi!

Sistemca čeka još formatiranje diska i reinstalacija Windowsa i svih korisničkih programa na inficiranom računalu, jer je to jedini siguran način uklanjanja Zepta. Brze konzultacije s kolegama pokazale su da se nakon nepotpunog uklanjanja nametnik brzo vraća i ponovo čini štetu. Bez pravog laba, izolirane sredine, ne isplati se riskirati.

Na kraju ostaju samo pitanja bez odgovora. Na primjer, zašto uređaj kupljen za filitriranje e-mailova nije zaustavio privitak sa Zeptom? Zašto je besplatni *clamav* otkrio gamad koju tri komercijalne verzije antivirusnog softvera nisu našle? Ti su komercijalni proizvodi "certificirani" za upotrebu u državnom i javnom sektoru. Što ako su izgubljeni dokumenti ustanovi toliko važni da je spremna platiti ucjenu? Jedan od razloga popularanosti Bitcoina je anonimnost transakcija, *coini* se prebacuju iz *walleta* u *wallet*, sve su transakcije zabilježene u glavnoj knjizi, ali su vlasnici *walleta* anonimni. Naknade za transakciju su male, pa emigranti koji se zaposle na zapadu tako šalju novac obitelji

doma u Bangladeš. Pošalju rodbini *smartphone* s instaliranom aplikacijom, da mogu plaćati trgovcima Bitcoinima, ili ih na bankomatima zamjenjivati za lokalnu valutu. Anonimnost osim sirotinji odgovara još i kriminalcima i teroristima, ali kažu da i obavještajne službe Bitcoinima financiraju svoje skrivene operacije. No naša država još živi u 19 stoljeću, nije nam dala u ruke alate za rješavanje problema 21. stoljeća. Sistemci tako žive u paralelnim svjetovima koji koegzistiraju, djelomično se preklapaju, ali uglavnom su odvojeni regulativnim barijerama. Tehnička znanja nisu dovoljna da bi sistemci mogli obavljati svoj posao najbolje što mogu, u najboljem od svih svjetova.

uto, 2016-09-13 12:29 - Aco Dmitrović**Kategorije:** Kolumna [1]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr./node/1676

Links
[1] https://sysportal.carnet.hr./taxonomy/term/71