Digitalni jaz in naše digitalne sledi

Milan Gabor, Inštitut za varnost podatkov in informacijskih sistemov (IVPIS), Viris

Povzetek — Digitalizacija sveta in nas samih je vedno večja, kar posledično pomeni, da puščamo vedno več digitalnih sledi. Naši podatki se hranijo v vedno več podatkovnih bazah in velikokrat se sploh ne zavedamo, da razni naši podatki ležijo marsikje. Pogoste ni samo težava pri nas, saj podatke posredujemo brez premisleka, ampak tudi pri zbirateljih in upravljavcih teh podatkov. Od skrbnikov omrežja in informacijskih sistemov je odvisno, kako dobro so ti naši podatki zaščiteni. V sklopu prispevka je izpostavljeno nekaj ključnih področij in primerov, kjer je možna njihova demonstracija.

Ključne besede — informacijska varnost, digitalna sled, podatek, varnost, sled

I. UVOD

Napredek Interneta, razvoj informacijskih storitev in naša vedno večja odvisnost od digitalnega sveta, so nas pripeljali tako daleč, da si življenja brez digitalnega jaza ne moremo več predstavljati. Že skoraj vsaka spletna stran hoče od nas imeti vsaj nekaj podatkov, ki so potem trajno zapisani v vsaj eno bazo, shranjeni vsaj v kakšnem arhivu in preneseni še na vsaj na eno drugo lokacijo. Večini spletnih strani je res dovolj samo naš elektronski naslov, druge se s tem ne zadovoljijo. Hočejo nam slediti, podtakniti piškotke, pridobiti čim več podatkov, čeprav si potem z njimi kaj dosti ne vedo ali nočejo pomagat. In ti podatki so potem zbrani na kašnem skupnem strežniku, kjer gostujejo s kopico drugih spletnih strani. Kakšen nivo varnosti te spletne strani zagotavljajo in kako ravnajo z našimi podatki je težko poizvedet. V primeru kakšnega uspešnega napada na gostujočo spletno stran na skupnem strežniku so ti podatki lahko tudi tarča napadalcev in kaj hitro se lahko zgodi, da se naši podatki znajdejo na kakšni strani vključno z našimi gesli, ki lahko da bodo celo v nekriptirani obliki.

II. KDO ME SPLOH SLEDI?

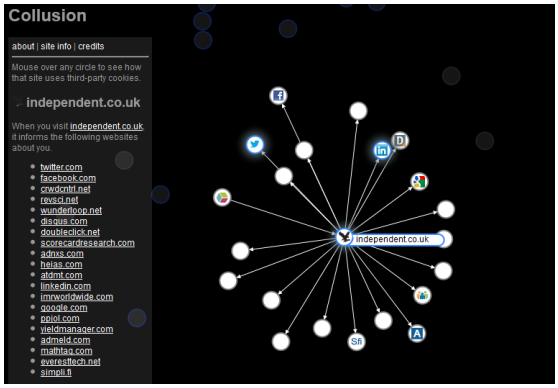
Torej ključno vprašanje pri tem našem digitalnem življenju, ki ga živimo v različnih spletnih aplikacijah, digitalnih sistemih, podatkovnih bazah, mobilnih aplikacijah je ta, kdo me sploh sledi. Odgovor je enostaven. Marsikdo nam sledi, čeprav se tega eksplicitno sploh ne zavedamo. Naj kot primer navedemo obisk spletne strani http://independent.co.uk/.

S posebnim dodatkom brskalniku Collusion [1] lahko sproti opazujemo, katera mesta nam poleg originalnih še sledijo. Ko odpremo spletno mesto, nam predvsem zaradi ciljnega oglaševanja sledijo ne samo tisto spletno mesto, ki smo ga odprli, ampak tudi dodatna spletna mesta, ki potem lahko spremljajo naše obnašanje, dolžino obiska in druge parametre, ki jih lahko sporoča naš brskalnik.

Prav zaradi tega se je sprožila iniciativa »Do not track« [2], ki bi uporabniku omogočala lastno izbiro pri tem spremljanju. Torej bi lahko uporabnik brskalniku povedal, da ne želi, da ga spletne strani spremljajo in brskalnik bi to posredoval strežniku. Nekateri brskalniki to opcijo že podpirajo, nekateri se nanjo še pripravljajo. Seveda je odvisno tudi od strežniške strani, da bo to uporabnikovo željo upoštevalo.

Zanimivo je tudi opazovati, da se je to sledenje oziroma če rečemo prestrezanje podatkov že tako zajedlo v naša omrežja, da je skoraj težko najti korporativno okolje, kjer se na primer ne bi prestrezali klici spletnih strani. Načeloma lahko obiski škodljivih strani povzročijo veliko škode in obstaja velika verjetnost, da se namesti kakšna škodljiva koda, vendar se poraja tudi vprašanje, kaj se s podatki o naših obiskih dejansko tudi dogaja in ali nas tudi kdo na tak način ne sledi in nadzoruje.

Debata in dileme na Twitterju informacijskega pooblaščenca nakazujejo na to, da tudi javna uprava ni na to imuna. In bolj kot to, da se nas ščiti pred neprimernimi stranmi in vsebinami, se poraja vprašanje, kaj pa se res počne s temi podatki, kako dolgo se hranijo in nenazadnje tudi kdo vse ima dostop do teh podatkov.



Slika 1: Primer obiska spletne strani

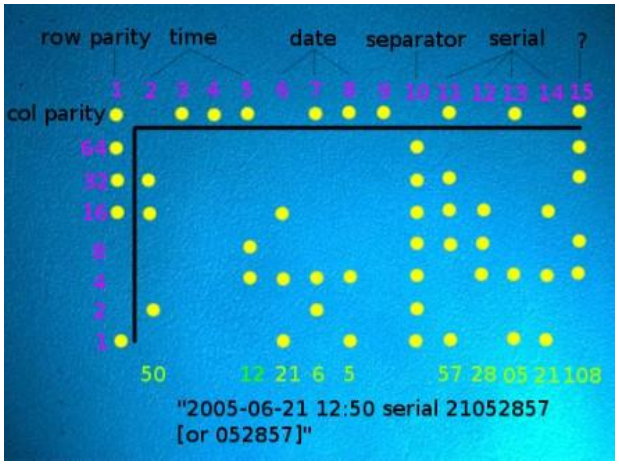
Slika 2: Primer prestreznika v javni upravi

III. DOKUMENTE SLEDI

Težko verjamemo, da se lahko vrnemo v svinčene čase, ko je vsak lastnik pisalnega stroja moral oddati vzorčni list, na katerem so bili odtisi vseh črk. S tem, so lahko preverili in tudi ugotovili, kdo je bil dejanski avtor spornih pisanj, ki bi lahko ogrožali takratno nacionalno varnost. Pa vendar po drugi strani, nekateri laserski pisalniki puščajo na vsakem odtisu strani skoraj nevidni vzorec točk, s kateri se lahko potem identificira tiskalnik, na katerem je bila stran natisnjena. Na strani so dodatno dodani še nekateri parametri, ki potem pomagajo pri določevanju izvora tiska. V ta primer se je vključila celo Evropska komisija, ki pravi, da je takšno sledenje mogoče celo kršitev človekovih pravic [3].

Za tiste malo bolj paranoične obstaja celo seznam tiskalnikov [4], ki teh oznak na tiskanih straneh ne puščajo.

Torej če povzamemo, lahko mala in skoraj nevidna kopica rumenih pik pove kdaj in na katerem tiskalniku je bil natisnjen dokument, ki ga mogoče trenutno držite v svojih rokah.



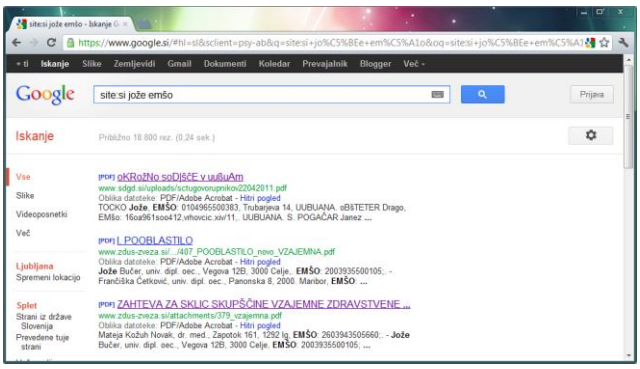
Slika 3: Prikaz skritega napisa v izpisu strani [5]

IV. ISKALNIK KOT NAJVEČJI SLEDILEC

S pojavo velikih iskalnikov, ki nepretrgoma preiskujejo spletni prostor, se je tudi povečal naš digitalni prstni odtis, ki ga puščamo na različnih spletnih straneh. In na drugi strani ni nujno, da so ti prstni odtisi vedno naši. Nekdo lahko na primer naloži naše dokumente ali dokumente v katerih se pojavljajo naši podatki brez naše vednosti. Ti podatki so lahko splošne narave, ki jih je mogoče najti v različnih javno dostopnih imenikih. Spletni brskalniki pa najdejo tudi takšne podatke včasih, ki niso javno objavljeni, kot na primer:

- EMŠO,
- davčne številke,
- neobjavljene privatne telefonske številke,
- pogodbe o sodelovanju.

Spletni iskalniki so postali pravi plenilci, saj pridno zbirajo podatke, informacije in dokumente o nas in o naših aktivnostih na spletu. In to počnejo takrat, ko mi to najmanj hočemo, kot na primer ko delamo nadgradnjo spletnih aplikacij in shranijo vse napake, ki se takrat pojavijo. Pridobijo podatke iz dokumentov, ki naj ne bi bili javni. In še eno lastnost imajo. Shranijo namreč podatke v svoje gromozanske medpomnilnike za nekaj časa in so na voljo tudi po tem, ko jih mi pobrišemo.



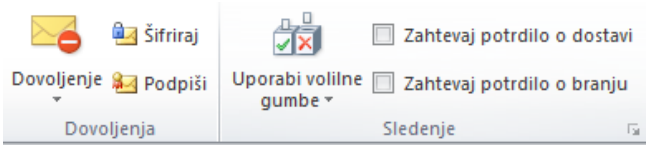
Slika 4: Prikaz pridobitve EMŠO podatkov

V. PREPROSTA SLED V ELEKTRONSKI POŠTI

Možnost sledenja se ne uporablja samo na Internetu in elektronskih storitvah. Na preprostem in banalnem primeru lahko pokažemo, da se da veliko informacij zbrati tudi že z uporabo bralnika elektronske pošte. Če pogledamo možnost, ki jo recimo ponuja Microsoft Outlook, lahko zahtevamo potrdilo o branju. Ta preprosta opcija, ki jo lahko izberemo za poljubno elektronsko sporočilo. Z izborom te opcije in v primeru, da naslovnikov odjemalec elektronske pošte to omogoča, lahko dobimo povratno sporočilo o tem, kdaj je naslovnik prebral naše sporočilo. Nekateri poštni odjemalci imajo kot privzeto nastavljeno opcijo, da tiho brez vednosti uporabnika pošljejo takšna sporočila o dostavi, ki pa lahko vsebujejo kopico uporabnih podatkov.

Z uporabo te opcije, lahko pridemo do pomembnih podatkov o okolju in storitvah naslovnika, brez da bi on karkoli o tem vedel. Tako lahko pridemo do naslednjih podatkov, vendar ne nujno vedno do vseh:

- Verzijo klienta ki jo uporablja,
- Internega IP naslova odjemalca,
- Interne IP naslove potovanja elektronskega sporočila,
- Tip internega strežnika za elektronsko pošto,
- Uporabljeno antivirusno zaščito in verzijo.



Slika 5: Prikaz možnosti zahtevka za potrdilo o branju

VI. DIGITALNE SLEDI NA DRUŽBENIH OMREŽJIH

Razmah družbenih omrežij v zadnjih nekaj letih je bil velikanski in veliko uporabnikov, se je pridružilo tem omrežjem in jih začelo uporabljati v vsakdanjem življenju. In spletna omrežja so postala pravi hit. Nekako v stilu, če te ni gor, ne obstajaš. In ta veliki bum, brez pravih navodil za pravilno in varno uporabo družbenih omrežij je krivec za kar nekaj neprijetnosti. Tako so se nekateri znašli pred praznimi stanovanji, ko so se vrnili z dopusta. Seveda so pred odhodom na dopust to javno objavili, prej še dodali nekaj fotografij stanovanj in opreme, ter morebiti pustili še kakšne naslov na katerem stanujejo. Spet drugi so bili zaradi svojih digitalnih sledi na družbenih omrežjih ob povišice in napredovanja ali celo ob službo. Tudi njihovi nadrejeni so spoznali moč družbenih omrežij in nespodobnih fotografij ter

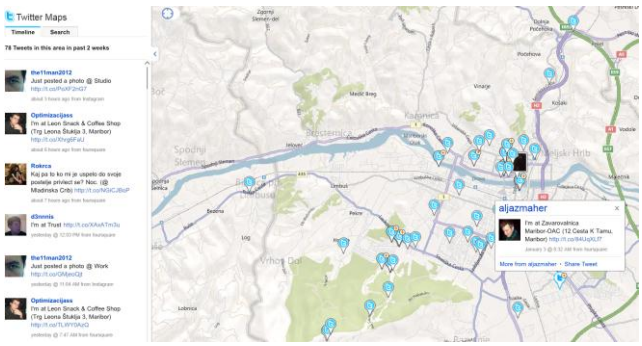
označevanja posameznikov, še posebej v rahlo kočljivih pozah.

Tako lahko naše prijatelje na primer spremljamo v vseh njihovih aktivnostih in to skoraj v realnem času ali z vsaj minimalnim zamikov nekaj sekund ali minut. In to sledenje omogočajo taisti uporabniki sami in to brez prisile.

Slika 6: Prikaz podrobnosti teka mojega prijatelja

Že prej omenjeni iskalniki lahko funkcije socialnih omrežij združijo in dodajo nova orodja, ki se jih lahko potem s pridom uporabi. Takšen primer na primer omogoča spletni iskalnik Bing. Z uporabo njegovega iskanja bo Bing Maps, lahko kot iskalni kriterij vnesemo tudi poljubno lokacijo. Tako lahko na primer pokaže vse, ki so tweetali v Ljubljani. In sočasno se pokaže tudi njihova lokacija tweeta in vsebina tweeta. Kar je še zanimivo je to, da večina pametnih telefonov že kot privzeto uporabniku ob prvi nastavitvi ponudi, da se objavljajo tudi njegove GPS koordinate. S takšnim preprostim načinom sledenja lahko izkoristimo objavljene podatke, ki bi lahko potem služili kot podlaga za napad z uporabo socialnega inženirstva. Na tak preprost in enostaven način, lahko dobimo zelo dober vpogled na obnašanje in aktivnosti konkretnih uporabnikov. In to brez policijskih metod ali najemu detektiva, ki bi sledil naši tarči.

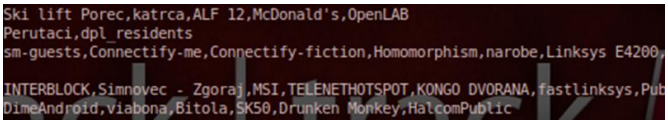
Koristni podatki, ki jih je mogoče dobiti:
- lokacije, kjer se nahaja uporabnik,
- kraji, kjer se zadržuje,
- posebni kraji, ki jih je obiskal (bolnišnice, zdravstveni domovi, drugi posebni kraji),
- prostor dela in domači naslov,
- seznam prijateljev, saj se pojavljajo na isti lokaciji.



Slika 7: Prikaz tweetov uporabnikov z njihovo lokacijo [6]

VII. BREZŽIČNO

Pametni telefoni ne nosijo zastonj imena pametni. Tako so namreč pametni, da med vsemi funkcijami, ki nam jih ponujajo omogočajo tudi to, da lahko zvemo, na katera vsa omrežja se je njihov lastnik prijavljal. Princip delovanja pri iskanju brezžičnih omrežij je tak, da se telefoni poskušajo povezati na tista omrežja, ki jih imajo shranjena in so bili že nekoč povezani nanje. S tem pa seveda izdajajo tudi vse SSID identifikatorje teh omrežij. In nekdo v pasivni vlogi, ki samo posluša prometu in glede tako imenovane beacon paketke v katerih se ti SSID tudi prenašajo, lahko v določenem časovnem intervalu ugotovi katere vse SSIDe je zahteval določen telefon. Nekdo bi rekel, nepomembna informacija, vendar s pravo kombinacijo analize vseh omrežij in lociranjem, kjer se ta omrežja nahajajo, lahko pridobimo približne lokacije določenega posameznika, kljub temu, da ga mogoče sploh ne poznamo. Če pa SSID razkrivajo recimo imena in priimke, restavracije, kampe, hotele, službe ali kakšne druge informacije, pa so takšne informacije še kako pomembne in seveda spet lahko služijo kot dobra podlaga za napad na uporabnika.



Slika 8: Prikaz iskanih SSIDov

VIII. ZAKLJUČEK

Kot je mogoče videti na nekaj primerih je naše digitalno in v določenih primerih tudi papirnato ali telefonsko življenje precej nadzorovano. Torej za tiste, ki imajo interes, je mogoče podatke o nas zbrati na kar nekaj različnih načinov, ki ne potrebujejo specifičnega in ekspertnega znanja. Tudi oprema za to izvedbo je precej dostopna. Nekateri podatki nam uhajajo celo brez naše vednosti in kontrole, kar je še toliko slabše. Zato je potrebno naslednjič, pred kakršnokoli objavo, dvakrat premisliti, ali so podatki, ki jih objavljamo res za objavo.

LITERATURA

[1] http://www.mozilla.org/en-US/collusion/
[2] http://en.wikipedia.org/wiki/Do_Not_Track
[3] http://seeingyellow.com/
[4] https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots
[5] https://w2.eff.org/Privacy/printers/docucolor/
[6] www.bing.com/maps/

Milan Gabor je direktor in lastnik podjetja ViRIS, katerega primarna dejavnost je razvoj in varnost informacijskih sistemov. Po večletnem delu kot razvijalec programske opreme, se je odločil za samostojno pot podjetnika in se preusmeril v informacijsko varnost in z njo povezanimi storitvami. Aktivno sodeluje v raziskovalni skupini v podjetju in pripravlja raziskovalne članke ter predavanja in delavnice s področja informacijske varnosti.