Spy web

Ubrzani razvoj Mreže donosi u prvi plan nove funkcionalnosti, neke željene, druge baš i ne. Pisali smo kako je Internet postao Money Web. Nekoliko naizgled nevezanih vijesti koje su mediji prenijeli ovih dana potakli su nas da još jednom razmislimo o novim funkcijama, a jedna od njih je "špijuniranje", odnosno manje ili više (i)legalno prikupljanje informacija.

Tri istraživača sa sveučilišta Princeton objavili su rezultate istraživanja o prikupljanju informacija o posjetiteljima web stranica. Rezultat je više nego zanimljiv: 482 od 500 najposjećenijih stranica koristi analitičke funkcije nezavisnih tvrtki (tzv. treće strane) koje se ponašaju kao ***keyloggeri***, što znači da bilježe i šalju velikom gazdi sve što korisnici tipkaju i sve pokrete miša za vrijeme dok im je otvorena posjećena web stranica. Wow!

Zamislite da gledate recept za jelo koje želite pripremiti za ručak, a usput se logirate na stranicu na kojoj obavljate neke povjerljive poslove, na primjer web bankarstvo, ili tražite informacije o bolesti koju su vam nedavno dijagnosticirali. Analitika s kulinarske stranice presreće URL, korisničko ime, password, ključne riječi po kojima pretražujete web, stranice koje otvarate... Zvuči zastrašujuće. Zar je moguće da je tako jednostavno zloupotrebljavati povjerenje ljudi koji surfaju?

Istraživači su podigli svoje web servere na kojima su aktivirali analitičke funkcije sljedećih tvrtki: Yandex, FullStory, Hotjar, UserReplay, Smartlook, Clicktale, SessionCam. Odabrali su ih zato jer se te usluge koriste na 482 sitea koje Alexa svrstava među najposjećenije. U fokusu su im bile takozvane ***replay skripte*** koje bilježe korisnikov unos. One odreda nude automatsko ili manualno postavljanje filtera koji bi trebali osigurati da ne primjer passwordi ili brojevi kreditnih kartica ne snimaju. Ispitujući rad tih skripti ustanovili su da se njihovo ponašanje razlikuje od deklariranog. Evo njihovih zaključaka:

- Passwordi su ponekad uključeni u snimku sesije (čini se da automatski filteri u nekim slučajevima ne rade dobro).
- Filtriranje osjetljivih informacija nije potpuno (na primjer FullStory zapisuje broj kreditne kartice, ali ne i tajni CC broj kojim se ovjerava plaćanje).
- Ručna konfiguracija filtera za svaku pojedinu stranicu je u osnovi nesigurna (trebalo bi provjeriti svaku stranicu posebno, zadati pravila i postupak ponavljati nakon svake izmjene na stranici)

Proizvođači analitičkog softvera obećavaju lakoću, sve će raditi odmah nakon instalacije. Ali bez ručnog podešavanja gotovo je sigurno da će povjerljivi podaci curiti, što tvrtke koje na svojim stranicama koriste analitiku stavlja u nezgodnu situaciju, jer korištenjem softvera treće strane mogu ugroziti vlastita pravila o čuvanju osobnih podataka i time se izložiti problemima. Na kraju krajeva, pitanje je koliko i njima samima odgovara kršenje naše privatnosti? Tako se na web ušuljala nova vrsta usluge: ***Keylogger as a service***.

Radoznalci mogu cijeli izvještaj pročitati na adresi: https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/ [1] . Tu će pronaći i link na web siteove koji koriste ***replay skripte***, kako bi ih mogli izbjegavati.

Druga vijest kaže da je Ministarstvo obrane Indije objavilo listu od 42 mobilne aplikacije za koje smatra da su potencijalno opasne. Radi se kineskom softveru, instaliranom na pametnim telefonima

kineskog porijekla, ali ih i korisnici uređaja drugih proizvođača mogu instalirati. Indijske obavještajne službe napravile su analizu i zaključile da taj spyware šalje informacije serverima u Kini, pomoću kojih bi se mogao otkriti raspored jedinica, na primjer. Pograničnim trupama je zabranjeno koristiti mobitele tvrtki Huawey i ZTE.

Evo popisa rizičnih aplikacija: Weibo, WeChat, SHAREit, Truecaller, UC News, UC Browser, BeautyPlus, NewsDog, VivaVideo- QU Video Inc, Parallel Space, APUS Browser, Perfect Corp, Virus Cleaner (Hi Security Lab), CM Browser, Mi Community, DU recorder, Vault-Hide, YouCam Makeup, Mi Store, CacheClear DU apps studio, DU Battery Saver, DU Cleaner, DU Privacy, 360 Security, DU Browser, Clean Master – Cheetah Mobile, Baidu Translate, Baidu Map, Wonder Camera, ES File Explorer, Photo Wonder, QQ International, QQ Music, QQ Mail, QQ Player, QQ NewsFeed, WeSync, QQ Security Centre, SelfieCity, Mail Master, Mi Video call-Xiaomi, and QQ Launcher.

Možda ćete poželjeti provjeriti na svom mobitelu je li neka od tih aplikacija instalirana. Možda ćete je poželjeti deinstalirati. Ako to vam to proizvođač to dozvoljava, naravno.

Iz tvrtke Truecaller, čija je aplikacija na listi, ogradili su se od ovakvih interpretacija, izjavivši da su oni Švedska tvrtka, da njihov program nije malware, da su sve sporne funkcije isključene "by default" i korisnik mora sam dati dozvolu za njihovu aktivaciju. Kad telefon zvoni, većina bi ljudi htjela znati tko ih zove. To nije moguće ako pozivatelj nije u vašem imeniku. Tu uskače Truecaller, koji iz svoje globalne baze provjerava tko je vlasnik broja i savjetuje korisnike da li da prihvate ili odbiju poziv. No, zapitat ćete se, čemu onda dodatne špijunske funkcije, ako nisu dio ove deklarirane usluge? Zar to nije definicija Trojanca: program koji osim deklarirane funkcionalnosti nosi još i neke skrivene, nepoželjne? Osim toga, iz činjenice da je tvrtka registrirana u Švedskoj ne može se zaključiti da su joj stvarni vlasnici Šveđani, zar ne? :)

Zanimljivo je pri tom da se prstom upire samo u Kineze. Samo bi naivac pomislio da se druge tehnološke velesile ne ponašaju jednako!

Tako je holandski sud presudio da Microsoftovi Windowsi 10 krše Zakon [2] o zaštiti osobnih podataka, jer prikupljaju povijest surfanja bez znanja i pristanka korisnika.

S prstima u pekmezu uhvaćen je i HP, na čijim je prijenosnicima pronađen predinstaliran tvornički softver koji također šalje "telemetriju" proizvođaču.

Njihove PR službe imaju spremne odgovore: oni poštuju privatnost korisnika, a podatke skupljaju samo radi poboljšanja usluge. :)

Kao zaključak ove priče može se lijepo iskoristiti razmišljanje koje iznosi izumitelj World Wide Weba, Tim Berners-Lee u članku "3 dark trends that could destroy the web [3]"

Lee izražava zabrinutost za budućnost weba, upozoravajući da se moramo pozabaviti s tri nova trenda koji prijete da će spriječiti web "da ostvari svoj potencijal alata u službi čovječanstva".

- **Izgubili smo kontrolu nad osobnim podacima**

Prevladavajući poslovni model je nuđenje besplatnih usluga u zamjenu za osobne podatke. Mnogi pristaju na to, ne shvaćajući da se ti podaci drže u "silosima" koji su posve izvan nadzora. Nitko nas ne pita da li želimo da se ti podaci dijele, tko će im pristupati i u koje svrhe, a nećemo dobiti ni dio potencijalne zarade koja se prodajom naših podataka može ostvariti. Osim tvrtki koje zanima zarada, naši su podaci primamljivi i državama, pogotovo represivnim režimima koji žele sve kontrolirati, pa čitamo o progonu ljudi koji su naivno povjerovali da na Internetu vlada sloboda govora i mišljenja.

- **Previše je lako koristiti web za širenje dezinformacija**

Većina koristi svega nekoliko siteova preko kojih tražimo sadržaje. Oni prate naše ponašanje i serviraju nam sadržaje u skladu s onim što oni misle da mi želimo. To se može koristiti da nam se

serviraju lažne vijesti i poluistine koje ćemo lako prihvatiti jer odgovaraju našim predrasudama.

- **Prikriveno političko oglašavanje traži veću transparentnost i razumijevanje**

Politički marketing je naglo postao sofisticirana industrija. Na izborima 2016. samo je preko Facebooka korisnicima servirano 50.000 varijacija oglasa prilagođenih individualnim profilima, odnosno na način na koji će ih pojedinac lakše "progutati". Neke su prakse izrazito neetične, na primjer kada se djeluje na ciljane grupe da ne izađu na izbore. Ovo nam zvuči poznato, zar ne?

Lee shvaća da neće biti lako riješiti ove probleme, ali nudi neka tehnička rješenja. Treba razviti nove tehnologije, na primjer organiziranje "čahura", "kapsula" koje čuvaju osobne podatke i omogućuju kontrolu pristupa. Korisnik bi bio upozoren na to da netko pokušava pristupiti njegovim podacima, mogao bi odbiti, dozvoliti, tražiti nešto zauzvrat itd. U isto vrijeme trebat će obeštetiti tvrtke koje pružaju servise, plaćati im usluge pretplatom ili "mikroplaćanjima" za povremeno korištenje, kako ne bi bili u napasti da traže polulegalne i ilegalne načine zarade. Nema tehničkih rješenja protiv vlada koje previše zadiru u privatnost građana, često pokrivene zakonima koji dozvoljavaju nadzor u ime nacionalne sigurnosti. U borbu protiv dezinformacija treba uključiti mjesta gdje se one objavljuju (FB i Google na primjer).

Lee nas poziva da se aktivno uključimo u ovu borbu, da podržimo Web Foundation i lokalne organizacije koje se zalažu za "digitalna prava". Ako vas je ovo zaintrigiralo, na kraju njegova članka [3] su linkovi. U svakom slučaju, lijepo je čuti da netko nastoji riješiti problem, umjesto pustog kukanja i pasivnog prihvaćanja svega što nas zadesi.

A što da radimo dok čekamo novu generaciju weba, koja će poštivati našu privatnost? Evo jednog prijedloga. Ne bi smjeli koirsiti isto računalo za neobavezno surfanje i za obavljanje ozbiljnog posla. Ako si ne možemo priuštiti dva fizička računala, nije teško podići jednu virtualku koju ćemo pokrenuti samo kad obavljamo povjerljive stvari, maksimalno je zaštiti vatrozidom, anonimizirajućim browserom itd. Sistemac može kod kuće odvojiti na routeru mrežu za ukućane od mreže za obavljanje posla. Itd. its. Može se, kad se hoće.

A kako se boriti protiv dezinformacija i pranja mozga? Za to nema tehničkog rješenja. Prije nego povjerujemo nekoj vijesti, promislimo kome je u interesu da prihvatimo poruke iz članka kao istinite? Zašto je vijest oblikovana baš tako, da nam se uvuče pod kožu bez aktiviranja sivih ćelija? Malo po malo razvit ćemo otpornost. Barem neki od nas.

sri, 2017-12-13 19:28 - Aco Dmitrović**Kategorije:** Kolumna [4]
Vote: 4.5

Vaša ocjena: Nema Average: 4.5 (2 votes)

story_tag: informacijska sigurnost [5]
privatnost [6]
prikupljanje osobnih podataka [7]

Source URL: https://sysportal.carnet.hr./node/1780

Links
[1] https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/

[2] https://techcrunch.com/2017/10/13/microsofts-windows-10-breaches-privacy-law-says-dutch-dpa/
[3] https://www.weforum.org/agenda/2017/03/three-challenges-for-the-internet-according-to-its-inventor
[4] https://sysportal.carnet.hr./taxonomy/term/71
[5] https://sysportal.carnet.hr./taxonomy/term/101
[6] https://sysportal.carnet.hr./taxonomy/term/84
[7] https://sysportal.carnet.hr./taxonomy/term/188