Otsin uksehoidjat: veebilehitsejad ja nende turvalisus

Kaido Kikkas

(Algselt avaldatud ajakirjas "30 pluss" juunis 2016, siin ilmub kokkuleppel toimetusega)

Üks jõukas inimene otsis kord uksehoidjat. Kohale tulid kolm kandidaati. Esimene oli ladna mees, jutt jooksis ja nägu oli naerul. Ent proovipäeval võttis ta lisaks peremehe külalistele lahkelt vastu ka mitu sullerit ja pätti - õhtuks oli trepikojast kadunud jalgratas ning postkasti sokutatud surnud rott. Teine kandidaat oli kantpäine endine sõjaväelane, kes paraku suutis lisaks sullerite edukale eemalepeletamisele ka külla tulnud vanatädile vihaselt peale karata ja tolle poolsurnuks ehmatada. Õnneks leidus ka kolmas, kes kaagid eemal hoidis ja head inimesed läbi lasi - tema võetigi tööle.

Meie arvutis on üheks selliseks uksehoidjaks veebilehitseja - see peab laskma veebist kõik hea ja kasuliku meieni, hoidma pahalased eemal ning tegema seda kõike sarnaselt heale uksehoidjale märkamatult. Võimalikke kandidaate on päris palju, ehkki tavakasutaja kipub sageli tundma vaid üht - seda, mis "arvutiga kaasa tuli". Tänases ohtuderohkes netimaailmas aga tasub sageli valida hea uksehoidja ning õppida teda ka hästi tundma.

Seinast seina

Veebis käimiseks on loodud kenake hulk tarkvara ning siintoodud loend ei ole kaugeltki mitte ammendav. Esmalt mõned suuremad ja tuntumad:
* Alustuseks Microsofti veebilehitsejad - kauane valitseja Internet Explorer ja selle järeltulija Edge (paljud arvutivõhikud on arvanud, et töölaual olev e-tähega ikoon tähendabki Internetti...). Oma hiilgeaegadel sajandivahetuse paiku oli Microsofti käes ligi 95% veebilehitsejate turust, siis aga jäädi loorberitele puhkama ja tehnoloogiliselt ajast maha. Microsofti veebilehitsejad on tänini saadaval vaid nende endi operatsioonisüsteemidele (tõsi, entusiastid on suutnud IE eri versioone ka Linuxitel käivitada ning mõnda aega pakuti IE variante ka Apple'i ja Unixi platvormidele).
* Apple'i süsteemides (OS X arvutitel ja iOS mobiilidel) on kasutusel Safari, mis on suurtegijatest ilmselt kõige rohkem enda nišis kinni (vahepeal oli küll saadaval ka Windowsile, ent alates 2012. aastast piirdub leviala taas vaid Apple'i süsteemidega). Samas on tegu kvaliteetse tarkvaraga.
* Vaba tarkvara maailma kauaaegne esinumber Mozilla Firefox on küll teenekas ja hea lehitseja, laia platvormivaliku (Windows, OS X, Linuxid, mobiiliplatvormid) ja väga suure lisamoodulite arvuga, kuid tänaseks on tema turuosa kahanenud - ühelt poolt on mõju avaldanud suure turujõuga Google'i mängutulek, samas aga tuleb osa süüst panna ka tegijate mõnedele küsitavatele valikutele.
* Opera on ilmselt vanim elusolev "nišibrauser", millel on oma kindel kasutajaskond. Mitmete hiljem laialt levinud uuenduste sissetoojana (sakkidega lehitsemine, privaatrežiim, laiendused) on tal veebi ajaloos kindel koht. Algselt vaid Windowsile mõeldud, on ta tänaseks levinud kõigile tuntumatele platvormidele.
* Google'i turujõu toel tänaseks valitsejaks kerkinud Chrome (Windowsi ja Apple'i süsteemides ning mobiilides) ja selle vabatarkvaraline teisend Chromium (eeskätt Linuxitel) on Firefoxilt juhtrolli üle võtnud - paljuski seetõttu, et on suudetud luua pea samaväärne lisamoodulite toetus ja samas vältida mitmeid konkurentide eksisamme.

Lisaks suurtele on aga olemas mitmeid projekte, mille nimegi paljud kuulnud ei ole. Näiteks
* Torch (http://www.torchbrowser.com/) - Chromiumi põhjal loodud veebilehitseja, mida on kiidetud töökiiruse ja sisseehitatud torrentikliendi eest. Samas on tegu reklaamvaraga, mis võib kasutamise tüütuks muuta, samuti on Torch saadaval vaid Windowsile.

* Seamonkey (http://seamonkey-project.org/) - "vana kooli värk", kunagise tipptegija Netscape'i järeltulija. Plussiks on sarnaselt esivanemaga terve komplekt rakendusi (lisaks veebilehitsejale ka e-postitarkvara, IRC ja Useneti klient ning veebiredaktor), samuti toetab SeaMonkey suurt osa Firefoxi laiendustest. Miinuseks on suurusest tulenev kohmakus ja aeglus.
* Epic (https://www.epicbrowser.com/) - esimene India päritolu veebilehitseja, mis põhineb Chromiumil ning paneb eraldi rõhku kasutaja privaatsusele (näiteks kustutab töö lõpetamisel kõik sessiooniandmed). Miinuseks on omandvaraline (ehkki tasuta) litsents ning esialgu saadavus vaid Windowsile ja OS X-ile.
* Comodo Dragon (põhineb Chromiumil; http://browser.comodo.com/) ja Ice Dragon (põhineb Firefoxil; http://icedragon.comodo.com/) - tuntud turvatarkvarafirma Comodo loodud teisendid kahele tuntud brauserile, eesmärgiks taas suurem privaatsus ja turvalisus. Samas on teada ka nendes esinevaid uusi turvaprobleeme.

Mis toimub veebilehitsejas

Esmalt tuleks meenutada üht lihtsat tõsiasja - veebi lehitsemine tähendab info kopeerimist veebiserverist lugeja arvutisse. Mis sealt lisaks ekraanil nähtavale sisule veel kaasa tuleb, selle reguleerimine ongi veebilehitseja üks olulisi ülesandeid. Nii nagu vorsti puhul võib selle koostise teadasaamine vorstiisu ära võtta, nii võib ka mõne veebilehe tegevus meie arvutis olla üsna ebameeldivalt üllatav.

Küpsised (*cookie*) on väikesed infojupid, mida paljud veebilehed meie arvutitesse sokutavad. Nad on väikesed ja üldjuhul märkamatud ning paljudel juhtudel aitavad tõsta kasutusmugavust (näiteks peavad arvet, milliseid alamlehti oleme juba külastanud). Samas on küpsiseid võimalik ka eri viisidel kurjasti kasutada.
Skriptid on erinevad programmid, mida veebileht käivitab - üheks lihtsaks näiteks võib tuua valuutakursi kalkulaatori panga veebilehel. Üldjuhul on neid kaht sorti:
* serveripoolsed - programm käivitatakse veebiserveris ja kasutaja näeb vaid töö tulemust
* kliendipoolsed - programm laetakse koos veebilehega meie veebilehitsejasse ning käivitatakse meie arvutis.
Sarnaselt küpsistega võib skriptimine olla nii hea- kui pahatahtlik. Eriti kurja näitena võib tuua nähtuse nimega XSS (*Cross-Site Scripting*), mis tähendab olukorda, kus süsteemi vigade tõttu saab programm "toppida oma nina võõrasse majja" ehk mõjutada otseselt teises arvutis toimuvat.

Mozilla perekonna veebilehitsejates on juba kaua aega kasutusel laiendus nimega NoScript (https://noscript.net/), selle variant NotScripts (Chrome/Chromium ja Opera) on kahjuks tänaseks tegevuse lõpetanud. Põhimõte on lihtne: vaikimisi keelatakse kõigi veebisaitide skriptid, usaldusväärsete kohtade omad saab püsivalt lubada ning kahtlasemate puhul saab neid lubada vaid ühekordselt. Et aga enamik skripte kasutavaid veebilehti ei näe nende keelamisel päris samamoodi välja, siis lisab see muidugi kasutajale tööd (skriptide lubamiseks tuleb paar lisaklõpsu teha).

Enamik veebilehitsejaid talletab surfamise ajaloo ning viskab kord juba külastatud aadressi alguse sisestamisel kogu aadressi ekraanile. Ühelt poolt on see mugav, teisalt aga taas privaatsusrisk, mistõttu ohutum oleks ajaloo salvestamine sätetest välja lülitada (korduvalt vajaminevate veebiviidete jaoks on olemas nii järjehoidjad kui paljudel lehitsejatel võimalus salvestada need tööriistaribale).

Nagu eespool öeldud, kopeeritakse loetav veebileht lehitseja vahemällu (*cache*) ning see säilib seal mõnda aega. Jällegi võib see teatud juhtudel privaatsusrisk olla - väidet "ma pole seal käinud" saab vahemälu abil ümber lükata küll.

Kõigil uuematel veebilehitsejatel on olemas privaatrežiim (irvhambad kutsuvad seda "pornorežiimiks"), mille kasutamise korral ei salvestata ajalugu, küpsiseid ega vahemälu. Tänaseks on see juba mitmeid aastaid kasutusel kõigis levinud veebilehitsejates ning võimaldab tavatasemel suuremat privaatsust. Samas ei ole see nähtamatuks tegev sõrmus - seda võivad takistada mitmed asjaolud, sh veebilehitsejasse paigaldatud laiendused. Kuna veebilehitsejad näitavad tava- ja privaatrežiimi korral mitmeid asju erinevalt, siis on võimalik loetaval veebisaidil tuvastada, kumba režiimi külaline parasjagu kasutab.

Lisalugemiseks soovitaks
* http://cybersecurity.ncb.mu/English/Documents/Knowledge%20Bank/Guidelines/Guideline%20For%20Securing%20Your%20Web%20Browser.pdf - Mauritiuse CERTi põhjalik juhis 2011. aastast (mõned uuemad asjad on puudu, kuid põhiosas pädeb see dokument ka täna).
* https://www.gov.uk/government/collections/browser-security-guidance - samalaadne dokument Suurbritanniast, pärit 2014. aastast.
* https://www.us-cert.gov/publications/securing-your-web-browser - samalaadne dokument USA-st, värskeim redaktsioon pärineb 2015. aastast.
* http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Veebilehitseja%20turvaline%20kasutamine.pdf - Andmekaitse Inspektsiooni juhendmaterjal lapsevanematele 2013. aastast.

Mõned soovitused

Alljärgnevad näpunäited kehtivad üldjuhul pea kõigi veebilehitsejate kohta:
* Nagu üldiselt arvuti kohta kehtib reegel "tea, milline tarkvara seal on", nii kehtib veebilehitsejates "tea, millised laiendused on sinna paigaldatud".
* Kui veebilehitseja seda toetab, lülita sisse kasutaja jälitamise keelamine ("Do Not Track").
* Võimalusel kasuta alati veebilehitseja privaatrežiimi.
* Võimalusel kasuta alati turvaühendust (HTTPS). Chrome, Firefox ja Opera saavad kasutada vastavat lisamoodulit (HTTPS Everywhere).
* Võimaluse korral ära salvesta paroole veebilehitsejasse. Kui seda siiski teha, tuleks kasutada ülemparooli - s.t. lehitseja küsib kõigil juhtudel üht (loodetavasti hästi valitud) parooli ning täidab seejärel parooliväljad meeldejäetud paroolidega.
* Ehkki surfamisajalugu võib olla saitide korduvkasutamisel mugav (aadressi ei pea tervenisti sisestama), on selle mittesäilitamine turvalisuse mõttes arukas tegu.
* Tasub kaaluda Google'i otsingu asendamist DuckDuckGo või mõne muu privaatsust paremini arvestava teenusega.
* Skriptide vaikimisi keelamine veebilehitsejas võib tunduda liigne ettevaatus, aga see on väga paljude sigaduste vastu väga tõhus abinõu.
* Hea lihtne (aga natuke tülikas ja natuke aeglane) abinõu on kasutada kahtlasemate veebi-nurgataguste külastamiseks kirjutuskaitstud andmekandjalt käivituvat operatsioonisüsteemi ja sealset veebilehitsejat. Selleks sobib hästi mistahes levinum Linuxi variant.
* Ja loomulikult on olemas Tor Browser (https://www.torproject.org/). Aga sellest (ja kogu tumeveebist ehk veebi varjatud osast) tuleb lähiajal eraldi juttu.

Kokkuvõtteks

Nagu mistahes kauba või teenuse valikul on ka veebilehitseja puhul oluline kasutaja teadlikkus. Mitmetes laiatarbe-operatsioonisüsteemides on kasutaja privaatsus jäetud tahaplaanile või tegeleb koguni tarkvara looja ise aktiivselt privaatsuse rikkumisega. Selle vastu aitab ühe olulise komponendina veebilehitseja teadlik valik, selle teadlik häälestamine ning muidugi teadlik kasutamine. "See tuli arvutiga kaasa" ja "Mida ma siin ikka muuta oskan" ei ole vabandused.

Leidke endale sobiv uksehoidja!