EFF'S SURVEILLANCE SELF-DEFENSE

JINSI YA: KUEPUKA UDHIBITI MTANDAONI

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

https://ssd.eff.org/en/module/how-circumvent-online-censorship

*Hii taarifa kwa ufupi ya namna ya kuepuka udhibiti mtandaoni

Serikali, makampuni na watoa huduma za mtandao wakati mwingine wanatumia program kuzia watumiaji wao kuingia kwenye wavuti na huduma. Hii huitwa uchujaji mtandaoni na ni mfumo wa udhibiti au uzuiaji. Uchujaji huu unaweza kuja katika sura mbalimbali. Kuna kuzuia ukurasa wa mtu mmoja mmoja au wavuti nzima. Wakati mwingine maudhui hufungiwa kwa maneno ya msingi.

Kuna njia mbalimbali za kupambana na udhibiti wa mtandaoni. Baadhi zinakulinda kutofuatiliwa lakini nyingi haziwezi. Iwapo kuna mtu anakufuatilia mtandao wako kwa kuuchuja au kuufunga unaweza kutumia hizi zana za kupinga ili kupata taarifa unayoitaka. Zingatia kuwa zana za uthibiti ambazo zinazoweza kuahidi usiri au usalama si lazima ziwe za kibinafsi na salama. Zana hizo zinzatumia maneno kama “asiyefahamika” sio kila wakati zinatunza utambulisho wako kama siri moja kwa moja.

Zana hizi za udhibiti ambazo zinaweza kuwa nzuri kwako zitategemea na vitu hatarishi ulivyonavyo. Kama hauna uhakika wa nani ni tishio kwako anza hapa... Makala hii itazungumzia njia nne za kupambana na udhibiti:

- Tembelea proxy ya wavuti kuona wavuti zilizofungiwa.
- Tembelea wavuti proxy ya usibaji fiche ili uweze kuona wavuti iliyofungiwa kwa kutumia VPN ili kupata wavuti iliyofungiwa au huduma iliyofungiwa.
- Tumia kivinjari TOR ili kuweza kupata wavuti zilizozuiwa au kukinga utambulisho wako.

Mbinu mahususi

Zana za kuepusha udhibiti huwa zinafanya kwa kuchepusha wavuti yako na kuepuka talakilishi ambao zinazuia au kuchuja.Huduma ambayo inayoongoza unganisho la inteneti itavyopita kwenye hivi vikwazo inaitwa proxy.

HTTPS indio toleo salama ya protocali ya HTTPS unalitumia kupata wavuti yako. Wakati mwingine kitambuzi inaweza kuzuia HTTP isiyo salama ya ukurasa wa mtandao. Hii inaamana kuwa unaweza kuupata tena ukurasa ulizuiwa kwa kuingiza toleo la anuani ya ukurasa huo kwa kuanza na neno HTTPS.

Hii inamanufaa iwapo zuio unalopigana nalo ni kwaajili ya wavuti binafsi hasa kwenye maudhui yake. HTTPs zinazuia wadhibiti kusoma trafiki ya wavuti na hivyo hawawezi kujua maneno muhimu ambayo nanayotumwa au kurasa za wavuti binafsi zinazotembelewa.

Wadhibiti wananaweza kuona jina la kikoa kwenye kila wavuti unayotembelea. Kwa mfano unatembelea “eff.org/https-everywher” hapa wadhibiti wanaweza kuona kupo hapo kwenye “eff.org” lakini sio kwenye ukurasav“https-everywhere”

Iwapo utagundua aina hii nyepesi ya kuwa kuzuia basi weka https:/ kabla hujainiga kwenye hicho kikoa cha http:

Kwa kufungua EFF's za HTTPS kila mahali ungani inakuwa moja kwa oja inabadilika kuwa HTTPS kila panapowezekana

Njia nyingine ambazo unaveza kuepuka misingi ya mbinu za udhibiti ni kujarimu kutumia jina na kikoa au URL kwa mfano badala ya kutembelea http://twitter.com, unaweza kujaribu kujaribu toleo rununu ya ukurasa wa http://m.twitter.com. Wadhibiti wanaotu zuina wavuti au kurasa za wavuti wanafanya kazi kwenye wavuti zilizozuiliwa na wavuti ambazo hazipo kwenye kundi lilizoiwa zitaweza kusonga mbele. Hawataweza kujua aina zote za wavuti na hasa kwa majina na hasa iwapo wasimamizi wa wavuti hizo watajua kuwa zimezuiliwa na wakasajili zaidi ya kikao kimoja.

Wakala wa mtadao

Wakata wa mtadao kama vile http:/proxy.org/) ni wavuti anayomwambia anamfanya mtumiaji aweze kuona wavuti nyingine zilizozuiwa. Hivyo ni njia nzuri ya kukwepa wadhibiti. Ili kuweza kutumia wakala wa mtandao tembelea wakala na uingize anuani ya wavuti kuona. Wakala atakuonyesha huo ukurasa unaoutafuta.

Ingawa wakala wa kimtandao anaota kinga ya aina yoyote lakini ipiwa itakuwa chagua bovu iwapo moduli tishio yako itakuwa ni pamoja na mtu anayeangalia vionganisho vyako vya intaneti. Hawa watakusaidia kutumia huduma zilizozuiliwa kama vile za kwenye mesagi. Wakala wa mtandao utakuwezesha kuwa na taarifa ya kila kitu iliyokamilika kuhusiana na jambo lolote unalifanya mtadaoni ambalo nitahitaji usiri na hivyo kwa watumiaji wengine itategemea na hali ya tishio ulilonalo.

Wakala anayejulikana

Mawakala tofauti wanatumia zana za kinga wanaongeza tabaka lingine la ulinzi kwenye yale yaliyopo ili kuweza kukwepa chujio. Muunganiko ambao umejulikana kwa wengine unaza usikione wewe kuwa unatembelea vikao vyao. Pamoja na kuwa wakala anayejulikana ni salama tofauti na vikoa ambavyo ni vya kimtandao yule anayetoa zana za ulinzi anaweza kuwa na taarifa zako. Wanaweza kuwa na jina na anuani yako ya emaili kwenye kumbukumbu zao. Hiyo inamanisha kuwa hizo zana za ulinzi zilizotolea hazina usiri wa moja kwa moja.

Njia nyepesi ya kutumia wakala wa mtadaoni ni ile inayoaanza na "https" hii itatumia wakala wa mtadaoni unatumiwa na wavuti. Ingawa unatahadharishwa kuwa watumiaji wa wakala hao wanaweza kuona data zako unazituma kwenye wavuti nyingine. Utrasurf na Psiphon ni mfano wa zana hizo.

Mtandao wa msibo fiche

Mremba wa wavuti binafsi (VPN) msimbo unatuma kumbukumbu zote za kupitia komputa nyingine. Komputa hii inaweza kuwa ni ya kibiashara au sioyokuwa ya kibiashara, kampuni yako au mtu mwingine anayeaminika. Pale ambapo huduma ya VPN inapokuwa imewekwa kwa usahihi unaweza kuitumia kufungua kurasa za wavuti, emeli, ujumbe, VoIP na huduma nyingine za kimtandao. VPN inalinda msafara wako wa kimtandao usiweze kudukuliwa lakini msambazaji wako wa VPN anaweza kutunza logo zako kwenye wavuti yako unaweza kuipata au kama mtu wa tatu

anaweza kuibia moja kwa moja kwenye mtandao wako. Inategemea na modeli ya tishio lako na hata serikali kukusikiliza kupita VPN yako au kukamata logo ya VPN yako inaweza kuwa ni hatari. Kwa watumiaji wengine hii inaweza kuongoa mafanikio ya muda mfupi ya faida za VPN.

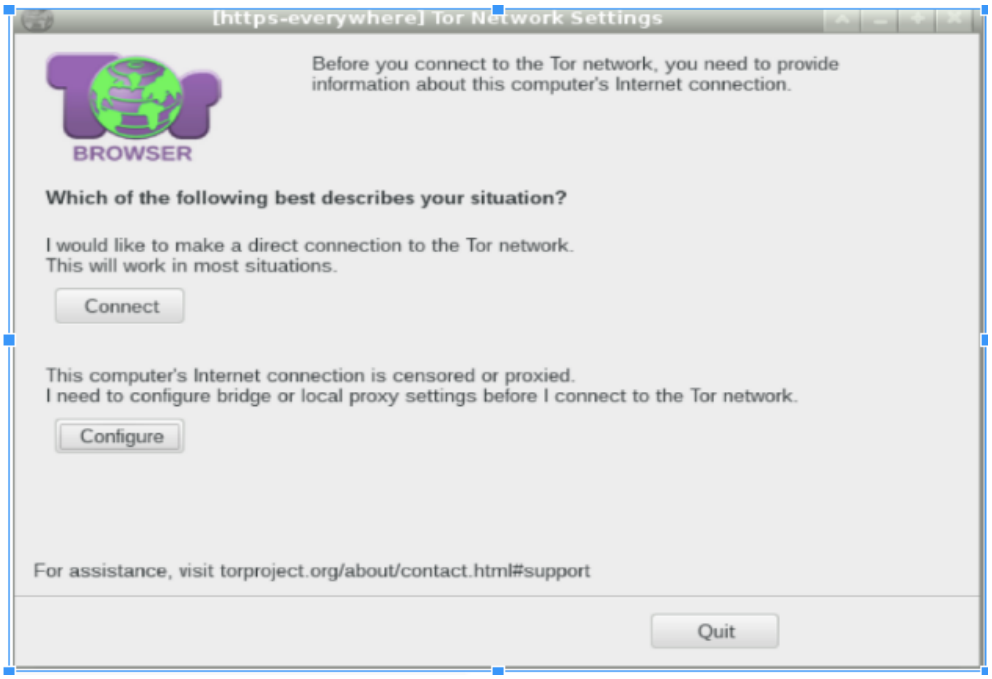
Kwa maelezo zaidi kuhusu VPN fungua hapa.

Sisi EFF hatuwezi kutumia kupima hii VPNs. baadhi ya VPSs ambazo zina sera binafsi zinaweza kuendeshwa na watu binafsi. Usitumia VPN ambazo haziaminiki.

Tor

Tor ni masijala ya wazi ya program ambayo imetengenezwa ili kukufanya usijulikane kwenye mtandao. Program ya Tor ni Tor ya kimtandao amabayo imejengwa juu ya Tor isiyojulikana. Hii ndio sababu Tor inaweza inaweza kuzuia udhibiti (angalia namna ya kutumia muongozo wa LINUX macOs na Windows).

Unapoanza kutumia kivinjari cha Tor unaweza kufanya chaguo mahususi kuonyesha kuwa uko kwenye mtadao ambao unadhibitiwa



Tor inaweza kupindisha karibu udhibiti wa mataifa yote lakini iwapo itakuwa imewekwa sawa sawa na pia inaweza kulinda utambulisho wako kwa maaduni au kusikilizwa kwenye mitandao ya nchi yako mwenyewe. Inaweza kuwa inakwenda pole pole na wakati mwingine ngumu kutumia.

Kujifunza namna ya kutumia Tor kwenye komputa yako ya mezani bonyeza hapa kwaajili ya Linux hapa kwaajili na macOs bonyeza haoa. Lakini hakikisha unabofya “Configure” badala ya “Connect (unganisha) kwenye displai ya windos kama inavyoonyeshwa hapo juu.