EFF'S SURVEILLANCE SELF-DEFENSE

JINSI YA: KUEPUKA MASHAMBULIZI YA UTAPELI DATA

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

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Katika harakati zako za kuboresha usalama wako wa kidijitali, unaweza kukutana na watendaji wabaya wanaojaribu kudhoofisha malengo yako ya usalama. Hawa watendaji wabaya tunawaita maadui. adui anapotuma barua pepe (au ujumbe mfupi wa maandishi au ujumbe katika programu) au kiungo ambacho kinaonekana kuwa kisicho na hatia, lakini ni hasidi, kinaitwa "utapeli data"

Shambulizi la utapeli data kwa kawaida huja katika mtindo wa ujumbe unaokusudiwa kukushawishi:

- kubofya kwenye kiungo
- kufungua waraka
- kusakinisha programu kwenye kifaa chako
- ingiza jina lako la mtumiaji na nenosiri kwenye wavuti ambao umeundwa kuonekana kuwa ni halali

Mashambulizi ya utapeli data kwa kawaida hutengenezwa ili kukuhadaa kupeana manenosiri yako au kukuhadaa ili usakinishe programu hasidi kwenye kifaa chako. Washambuliaji wanaweza kutumia programu hasidi kudhibiti kifaa chako, kuiba maelezo au kupeleleza ukiwa mbali.

Mwongozo huu utakusaidia kutambua mashambulizi ya utapeli data unapoyaona na kuelezea baadhi ya njia unazoweza kutumia ili kukusaidia kujilinda dhidi yao.

Ingawa tunazungumzia zaidi utapeli data wa barua pepe katika mwongozo huu, mbinu hizi hazizuiliwi kwa barua pepe tu; zinaweza kutumiwa kwenye simu, SMS, au katika programu zilizo na utendaji wa mazungumzo.

Aina za Mashambulizi ya Utapeli Data

Utapeli Data wa Manenosiri (unaojulikana kama Ukusanyaji wa Hati Tambulishi)

Matapeli wa Data hujaribu kukuhadaa ili upeane manenosiri yako kwa kukutumia kiungo kidanganyifu. Anwani za wavuti katika ujumbe zinaweza kuonekana kuwa na kusudio moja, lakini huelekeza kwa lingine. Kwenye kompyuta yako, unaweza kuona URL linalokusudiwa kwa kuelea juu ya kiungo. Lakini viungo vinaweza kufichwa zaidi kwa "herufi zinazofanana," au kwa kutumia majina ya vikoa ambayo vinatofautiana kwa herufi moja na majina halali ya vikoa na vinaweza kukuelekeza kwenye ukurasa wa

tovuti unaoonekana kwenda kwa huduma unayotumia, kama vile Gmail au Dropbox. Skrini hizi za kuingia zenye nakala bandia mara nyingi huonekana kuwa halali hivi kwamba inashawishi kuandika jina lako la mtumiaji na nenosiri. Ukifanya hivyo, utatuma kitambulisho chako cha kuingia kwa washambuliaji.

Kwa hivyo kabla ya kuandika nenosiri lolote, angalia upau wa anwani wa kivinjari chako cha wavuti. Utaonyesha jina halisi la kikoa la ukurasa. Ikiwa hailingani na wavuti unaofikiri kuwa unaingia, usiendelee! Kuona nembo ya shirika kwenye ukurasa hakuthibitishi kuwa ni halisi. Mtu yeyote anaweza kunakili nembo au muundo kwenye ukurasa wake ili kujaribu na kukuhadaa.

Baadhi ya matapeli wa data hutumia tovuti zinazofanana na anwani maarufu za Wavuti ili kukupumbaza: https://wwwpaypal.com/ ni tofauti na https://www.paypal.com/. Vile vile https://www.paypaI.com/ (yenye herufi kubwa "i" badala ya herufi ndogo "L") ni tofauti na https://www.paypal.com/. Watu wengi hutumia vifupisho vya URL ili kurahisisha kusoma au kuandika URL ndefu, lakini hizi zinaweza kutumika kuficha maeneo hasidi. Ukipokea URL iliyofupishwa kama kiungo cha t.co kutoka Twitter, jaribu kuiweka kwenye https://www.checkshorturl.com/ ili kuona inakuelekeza wapi.

Usimwamini mtumaji barua pepe, pia. Ni rahisi kughushi barua pepe ili zionyeshe anwani isiyo ya kweli ya kurejesha. Hii inamaanisha kuwa kukagua anwani ya barua pepe dhahiri ya mtumaji hakutoshi kuthibitisha kwamba barua pepe ilitumwa na mtu anayeonekana kutoka kwake.

Utapeli data unaolenga mtu mahususi (utapeli data wa sauti, utapeli data wa SMS, na kadhalika)

Mashambulizi mengi ya utapeli data huhusisha watu wengi. Mshambuliaji anaweza kutuma barua pepe kwa mamia au maelfu ya watu akidai kuwa na video ya kusisimua, hati muhimu, arifa ya usafirishaji au mzozo wa bili.

Lakini wakati mwingine mashambulizi ya utapeli data hulengwa kulingana na kitu ambacho mshambuliaji tayari anajua kuhusu mtu binafsi. Hii inaitwa "utapeli data unaolenga mtu mahususi." Fikiria umepokea barua pepe kutoka kwa Mjomba wako Boris ambayo inakuarifu kuwa ina picha za watoto wake. Kwa kuwa Boris ana watoto na inaonekana kama inatoka anwani yake, unaifungua. Unapofungua barua pepe, kuna hati ya PDF iliyoambatishwa. Unapofungua PDF, inaweza hata kuonyesha picha za watoto wa Boris, lakini pia inasakinisha programu hasidi kichinichini kwenye kifaa chako ambayo inaweza kutumika kukupeleleza. Mjomba Boris hakutuma barua pepe hiyo, lakini mtu anayejua una Mjomba Boris (na kwamba ana watoto) alifanya hivyo. Hati ya PDF ambayo ulibofya ilianzisha kisomaji chako cha PDF, lakini ilichukua fursa ya hitilafu

katika programu hiyo kuendesha msimbo wake. Zaidi ya kukuonyesha PDF, pia ilipakua programu hasidi kwenye kompyuta yako. Programu hasidi hiyo inaweza kupata wawasiliani zako na kurekodi kile kamera na maikrofoni ya kifaa chako huona na kusikia.

Njia nyingine ya utapeli data unaolenga mtu mahususi ni utapeli data wa sauti, ambapo ni kuhadaa ili kupata maelezo ya kibinafsi, ambapo mshambuliaji huiga mlengwa mahususi, ikiwezekana hata kufikia kuunda kloni ya Akiliunde ya sauti yake. Ikiwa sauti haitambuliki au inakuuliza mambo yasiyo ya kawaida kama vile pesa, waambie wathibitishe utambulisho wao kwa njia nyingine (kama vile kukuambia jambo ambalo ninyi wawili pekee mnalijua au kutuma ujumbe kutoka kwa akaunti nyingine).

Njia bora zaidi ya kujilinda dhidi ya mashambulizi ya utapeli data ni kutowahi kubofya viungo vyovyote au kufungua viambatisho vyovyote. Lakini ushauri huu haufai kwa watu wengi. Zifuatazo ni baadhi ya njia unazoweza kutumia kujikinga dhidi ya utapeli data.

Jinsi ya Kusaidia Kujikinga Dhidi ya shambulizi la Utapeli Data

Hakikisha Kwamba Programu Yako Imesasishwa Wakati Wote

Mashambulizi ya utapeli data ambao hutumia programu hasidi mara nyingi hutegemea hitilafu za programu ili kuweka programu hasidi kwenye mashine yako. Kwa kawaida mara tu hitilafu inapojulikana, mtengenezaji wa programu atatoa sasisho ili kuirekebisha. Hii inamaanisha kuwa programu ya zamani ina hitilafu zaidi zinazojulikana hadharani ambazo zinaweza kutumika kusaidia kusakinisha programu hasidi. Kusasisha programu yako hupunguza hatari za programu hasidi.

Tumia Kidhibiti cha Nenosiri kilicho na Kujaza Kiotomatiki

Vidhibiti vya nenosiri ambavyo hujaza manenosiri kiotomatiki hufuatilia tovuti ambazo manenosiri hayo yanamilikiwa. Ingawa ni rahisi kwa mwanadamu kudanganywa na kurasa bandia za kuingia, vidhibiti vya nenosiri havidanganyiki kwa njia sawa. Ikiwa unatumia kidhibiti cha nenosiri (ikiwa ni pamoja na kidhibiti cha nenosiri kilichoundiwa kwenye kivinjari chako), na kinakataa kujaza nenosiri kiotomatiki, unapaswa kusita na kuangalia tena tovuti unayotumia. Afadhali, tumia manenosiri yaliyoundwa nasibu ili ulazimike kutegemea kujaza kiotomatiki, na uwezekano mdogo wa kuandika nenosiri lako kwenye ukurasa bandia wa kuingia. Hata hivyo, kumbuka kwamba tovuti zinaweza (na kufanya) kubadilisha kurasa zao za kuingia, na wakati mwingine kufanya hivyo kunaweza kusababisha kujaza kiotomatiki kusifanyike ipasavyo, hata kwenye tovuti

halali. Ukiwa na shaka, nenda moja kwa moja kwenye ukurasa wa kuingia wa tovuti kutoka kwa kivinjari chako, si kwa kubofya kiungo katika ujumbe.

Thibitisha Baruapepe na jumbe za Maandishi na Watumaji

Njia moja ya kutambua ikiwa baruapepe au maandishi ni shambulizi la utapeli data ni kuangalia kupitia kituo tofauti na mtu ambaye anadhaniwa kutuma. Ikiwa barua pepe au maandishi yanadaiwa kutumwa kutoka kwa benki yako, usibofye viungo. Badala yake, pigia benki yako simu au fungua kivinjari chako na uandike URL ya tovuti ya benki yako. Vivyo hivyo, ikiwa Mjomba wako Boris atakutumia kiambatisho cha barua pepe kisicho cha kawaida, mtumie ujumbe mfupi na umuulize ikiwa alikutumia picha za watoto wake kabla ya kuifungua.

Fungua Nyaraka zinazotiliwa shaka katika Hifadhi ya Google

Baadhi ya watu wanatarajia kupokea viambatisho kutoka kwa watu wasiojulikana. Kwa mfano, waandishi wa habari kwa kawaida hupokea hati kutoka kwa vyanzo. Lakini inaweza kuwa vigumu kuthibitisha kuwa hati ya Word, lahajedwali ya Excel, au faili ya PDF si hasidi.

Katika visa hivi, usibofye mara mbili faili iliyopakuliwa. Badala yake, ipakie kwenye Hifadhi ya Google au kisoma hati kingine mtandaoni. Hii itageuza hati kuwa picha au HTML, ambayo kwa hakika itaizuia kusakinisha programu hasidi kwenye kifaa chako.

Iwapo unaridhishwa na kujifunza programu mpya, uko tayari kutumia muda kuweka mazingira mapya ya kusoma barua au hati za kigeni, na kupata barua pepe za kutosha za aina hizi ili kuhalalisha mahitaji ya muda wa ziada, fikiria kutumia mfumo maalum wa uendeshaji ulioundwa kuzuia athari za programu hasidi. Tails ni mfumo wa uendeshaji unaotegemea Linux ambao hujifuta wenyewe baada ya kuutumia. Qubes ni mfumo mwingine unaotegemea Linux ambao hutenganisha programu kwa uangalifu ili zisiingiliane, na kupunguza athari za programu hasidi yoyote. Zote mbili zimeundwa kufanya kazi kwenye kipakatalishi au kompyuta ya mezani.

Vilevile unaweza kuwasilisha viungo na faili zisizoaminika kwa VirusTotal, huduma ya mtandaoni ambayo hukagua faili na viungo dhidi ya injini mbalimbali za kinga-virusi na kuripoti matokeo. Hii si kwamba haina hitilafu —kinga-virusi mara nyingi hushindwa kutambua programu hasidi mpya au mashambulizi yanayolengwa—lakini ni bora kuliko kutofanya chochote. Hata hivyo, kumbuka kuwa faili au kiungo chochote unachopakia kwenye tovuti ya umma, kama vile VirusTotal au Hifadhi ya Google, kinaweza kutazamwa na mtu yeyote anayefanya kazi katika kampuni hiyo, au ikiwezekana mtu yeyote anayeweza kufikia wavuti huo, kama vile VirusTotal. Ikiwa maelezo yaliyomo kwenye faili ni nyeti au mawasiliano ya upendeleo, unaweza kufikiria njia mbadala.

Tumia Kitufe cha Universal 2nd Factor (U2F) wakati wa Kuingia

Nyavuti nyingine hukuruhusu kutumia cheti maalum cha maunzi chenye uwezo wa hali ya juu ili kuepuka majaribio ya utapeli data. Vyeti hivi (au "funguo") huwasiliana na kivinjari chako ili kupata vitambulisho kwa kila tovuti kwa ajili ya kuingia. Hii inaitwa Universal 2nd Factor au "U2F," kwa sababu ni njia ya kawaida ya kuhitaji mbinu mbadala ya uthibitishaji—pamoja fungu nywila yako—wakati wa kuingia. Unaingia kawaida kwa njia rahisi, na (unapoombwa) kuunganisha ufunguo kwenye kompyuta au simu maizi yako na ubonyeze kitufe ili uingie. Ikiwa uko kwenye tovuti ya utapeli data, kivinjari kitagundua kutokuingia na vitambulisho vilivyowekwa kwenye tovuti halali. Hii ina maana kwamba hata kama tapeli atakuhadaa na kuiba fungu nywila yako, hatahatarisha akaunti yako. Yubico (mtengenezaji mmoja wa funguo hizo) hutoa maelezo zaidi kuhusu U2F.

Hili halipaswi kutatanishwa na uthibitishaji wa vigezo viwili kwa ujumla, ambavyo vinaweza kutoa au kutotoa ulinzi dhidi ya utapeli data. Funguo nywila ni chaguo jipya zaidi la kuingia ambalo linaweza kutoa ulinzi dhidi ya utapeli data, na unapaswa kufikiria kulitumia linapotolewa. Ukiwa na funguo nywila, kivinjari chako kinatambua ni tovuti gani haswa inatumia ufunguo nywila fulani, na hakidanganyiki na tovuti bandia.

Kuwa Makini katika Maelekezo yaliyotumwa kwa Baruapepe

Baadhi ya baruapepe za utapeli data huadai kuwa zinatoka kwa idara ya usaidizi wa kompyuta au kampuni ya teknolojia zinakuomba ujibu kwa manenosiri yako, ili kuruhusu ufikiaji wa mbali wa "mtu anayerekebisha kompyuta" kwa kompyuta yako, au kuzima kipengele fulani cha usalama kwenye kifaa chako. Baruapepe hizi mara nyingi huwa na toni ya kusisitiza na hujaribu kutumia hofu kukuhadaa katika jambo fulani.

Kwa mfano, baruapepe inaweza kutoa maelezo yanayodaiwa kwa nini hii ni muhimu kwa kudai kuwa kisanduku chako cha baruapepe kimejaa au kwamba kompyuta yako imedukuliwa. Kwa bahati mbaya, kutii maelekezo haya ya ulaghai kunaweza kuwa hatari kwa usalama wako. Kuwa mwangalifu hasa kabla ya kumpa mtu yeyote data ya kiufundi au kufuata maelekezo ya kiufundi isipokuwa unaweza kuwa na uhakika kabisa kwamba chanzo cha ombi ni halisi. Kampuni nyingi hazitaomba kutatua shida yako. Kwa vyovyote vile, wanaweza kukutumia arifa kuhusu mabadiliko yajayo au kuzidiwa kwa data pamoja na kiungo cha hati za umma.

Ikiwa mtu atakutumia baruapepe au kiungo kinachotiliwa shaka, usiifungue au kukibofya hadi kudhibiti hali hiyo kwa vidokezo vilivyoorodheshwa hapo juu na unaweza kuwa na uhakika kwamba si hasidi.

Zima Picha za Nje katika Programu Yako ya Baruapepe

Picha zilizo ndani ya baruapepe zinaweza kutumika kufuatilia ni nani aliyefungua baruapepe na lini. Pengine umekumbana na haya mengi katika baruapepe za uuzaji, lakini zinaweza kuwa muhimu katika utapeli data, pia. Kwa hivyo, badala ya kuruhusu kila picha kupakiwa katika kila baruapepe kila wakati, ni vyema kuweka kiteja chako cha baruapepe—iwe hiyo ni programu kama Outlook au huduma kama vile Gmail—“Uliza kabla ya kuonyesha picha za nje.” Kwa kuweka chaguo hili, utahitaji kubofya chaguo katika kila barua pepe ili kupakia picha. Baadhi ya programu za barua pepe zinaweza pia kutoa hatua nyingine za faragha, kama vile programu ya Baruapepe ya Apple, ambayo hupakia picha zote kwa mbali kwa chaguomsingi.