Suur tarneahelarünnak: häkiti nii CNN-i, BBC-d kui Zoomi ja teisi

1 tund tagasi - 17.11.2026 Autor: AM

Esmaspäeval, 16. novembril, mil vähemalt 178 maailma suurimat organisatsiooni ja brändi jagasid oma pahaaimamatutele külastajatele pahavara. Ohvrite nimekiri on aukartustäratav: löögi alla sattusid teiste seas CNN, BBC, Zoom, Salesforce, GitLab, IKEA, HSBC, Equifax, Air France-KLM, krüptorahakottide tootja Ledger ning voogedastusplatvorm Peacock.

Rünnaku muudab eriti salakavalaks tõsiasi, et ühegi mainitud hiiu enda serveritesse ei murtud tegelikult sisse. Kurjategijad kasutasid ära turvaaugu populaarses veebianalüütika ja A/B-testimise platvormis Optimizely Web Experimentation, mille kaudu süstiti pahatahtlik JavaScripti kood otse klientide veebilehtedele laetavatesse skriptidesse.

Trooja hobune usaldatud teenusepakkuja serveris

Tänapäeva veebilehed ei ole enam ammu ühest tükist tahutud kivirahnud, vaid meenutavad pigem moodulitest kokku pandud legolinna, kus iga kolmanda osapoole teenus toob lehele oma väikese koodijupi ehk skripti. Kui üks selline usaldatud ehitusklots osutub mürgitatuks, nakatub hetkega kogu linn – ilma et majaomanik ise oleks ühtegi ust lukust lahti unustanud.

Optimizely töötab põhimõttel, et iga klient laeb oma veebilehele väikese koodijupi (inglise keeles snippet), mis asub Optimizely enda sisuedastusvõrgus (cdn.optimizely.com). See fail uueneb automaatselt iga kord, kui veebilehe haldaja oma töölaual seadeid muudab, ning sisaldab ka spetsiaalset välja nimega Project JavaScript, mis jookseb käima igal lehe laadimisel.

Veebilehtede skripte seirav turvafirma Report URI ja selle asutaja Scott Helme tuvastasid, et ründaja kirjutas oma pahavara laadija otse klientide Project JavaScripti väljale, jättes ülejäänud faili puutumata. Kuna kood serveeriti endiselt Optimizely ametlikust domeenist ja kehtiva turvasertifikaadiga, pidasid kõik veebilehed ja külastajate brauserid seda täiesti usaldusväärseks.

Teisipäeva varahommikul kell 01:02 UTC avaldatud teates kinnitas Optimizely, et ründaja "kasutas ära haavatavuse Experimentationi teenuses" ning lisas selle abil

mõnede klientide projektidesse pahatahtliku JavaScripti. Ettevõte küll eemaldas koodi ja turvas kontod, kuid jättis täpsustamata, kuidas ründaja nii paljudele omavahel mitteseotud projektidele ligi pääses.

Enne ametliku teate ilmumist tõdes Report URI oma analüüsis otsekoheselt, et nad ei tea, kuidas ründaja sai kirjutusõiguse nii paljudele võõrastele projektidele: "See jääb Optimizely selgitada." Kahtlusi ründaja püsivast ligipääsust süvendas asjaolu, et näiteks tarkvarafirma Smartsheet skript puhastati korra ära, kuid nakatati seejärel uuesti koodi peidetud (base64-kodeeritud) versiooniga. Kurioossel kombel olid nakatatud ka Optimizely enda pealeht ja sisselogimisleht.

Neli ühes: krüptovargusest iPhone'ide ründamiseni

Küberjulgeoleku uurijate poolt OPTIMJACK-iks ristitud kampaania laadis ohvrite seadmetesse faili nimega track.js, mida ehitati päeva jooksul ümber koguni 26 korda. See toimis kui mitmeotstarbeline digitaalne Šveitsi armee nuga, millel oli neli peamist ülesannet:

- Krüptorahakoti aadresside vahetamine: Skript otsis veebilehe tekstist, vormidest, linkidest ja väljuvatest päringutest kehtivaid krüptovaluutade (Bitcoin, Ethereum, TRON, Solana, Litecoin, Dogecoin jt) aadresse. Kui lehel esines maksetele viitavaid sõnu nagu wallet, deposit või send, vahetas pahavara aadressi märkamatult kurjategija oma vastu. Turvaline polnud isegi teksti kopeerimine: kui kasutaja kopeeris aadressi ajal, mil nakatatud vahekaart oli brauseris avatud, asendati see lõikelaual ründaja aadressiga.

- Pangakaartide koorimine (card skimming): Kell 13:43 UTC lisati koodile moodul, mis valvas veebivormide sisestusi ning haaras lennult kaardi numbri, kehtivusaja ja CVV-turvakoodi. Hea uudis on see, et eraldiseisvates turvaraamides (cross-origin iframe) asuvatele makselahendustele – nagu Stripe või Adyen – pahavara küüned taha ei ulatunud. Ohus olid vaid lehed, mille maksevormid asusid otse veebilehe enda koodis.

- Küpsiste ja ekraanipiltide vargus: Niipea kui pahavara vahetas lehel ära mõne krüptoaadressi, tegi see html2canvas tööriista abil kasutaja ekraanivaatest pildi ning saatis selle koos veebilehe küpsistega (välja arvatud HttpOnly märgistusega kaitstud sessiooniküpsised) ründaja serverisse.

- iOS-i ründekomplektid (Coruna ja DarkSword): Kui lehte külastati iPhone'i või iPadiga, laadis pahavara kahest .icu lõpuga domeenist lisaskripti boot.js. See tuvastas seadme operatsioonisüsteemi versiooni ja avas peidetud raamis vastava ründeahela: iOS 13 kuni 17.2.1 seadmetele suunati Coruna, iOS 18.4 kuni 18.7 seadmetele DarkSword ning iOS 26 puhul eraldi ahel, mis piirdus seadme andmete kogumisega. Vanematel kui iOS 18.6 seadmetel laadis nakatatud leht end iga 60 sekundi järel uuesti, et rünnakut korrata.

Õnneks ei ole seni märke, et ükski Apple'i nutiseade oleks rünnaku käigus päriselt üle võetud. Küberturbeplatvormi Cynet teadlased, kes uurisid teise etapi koodi emuleeritud iPhone'i brauseris, kirjeldasid nähtut kui tingimuslikku koodiedastust, "mitte füüsilise iPhone'i või iPadi edukat kompromiteerimist." Samuti märkisid ründekomplekti loojad ise oma koodi kommentaarides, et iOS 18.7.3 ja uuemad ning iOS 26.3 ja uuemad versioonid on turvapaikadega kaitstud.

Kui palju raha kurjategijad saagiks said?

Kuigi varastatud pangakaartide ja sessioonikūpsiste täpset hulka näevad vaid ründajad ise, on plokiahela tehingud avalikud. Report URI andmetel laekus esmaspäeva õhtuks kella 19:25 UTC seisuga kurjategijate krüptorahakottidesse umbes üheksa tunni jooksul ligikaudu 7040 USA dollarit (peamiselt Bitcoinis, Litecoinis ja USDT-s).

Teine turvafirma, StepSecurity, hindas samade aadresside kogusaagiks umbes 6600 dollarit. Kuna kaks rahakotti olid kasutusel juba enne Optimizely rünnaku algust, märkisid StepSecurity analüütikud oma raportis, et "plokiahel ei näita, millised ülekanded tulid ohvritelt." Küll aga selgus ajajoonest, et sama rühmituse varasem süstija (webshell.lol) ilmus esmakordselt Türgi veebilehtedele juba 17. septembril ning levis eelmise nädala lõpust saadik ka Kissmetricsi, StorifyMe ja Minute Media skriptide kaudu.

Teisipäeva, 17. novembri hommikuks olid kõik nakatatud Optimizely skriptid puhastatud ning ründajate peamised juhtserverid (1688360.cc ja webshell.lol) maha võetud.

Miks turvameetmed rünnakut kinni ei pidanud?

Report URI kontrollis 256 nakatunud organisatsiooni veebimajutust, et näha, kas sisuturbepoliitika (CSP – Content Security Policy) aitas rünnakut tõrjuda. Tulemus oli kainestav: vaid 24 lehekülge (15%) suutsid pahavara käivitumise täielikult

blokeerida.

Tervelt 68 organisatsioonil puudus CSP täielikult ning 50 lehel lubas seadistus nii pahavara jooksutamist kui ka andmete väljasaatmist. Isegi karmid reeglid vedasid alt, kui kasutusel olid seaded 'strict-dynamic' (mis usaldab automaatselt kõiki skripte, mida usaldatud Optimizely skript ise edasi laeb) või 'unsafe-eval', mida Optimizely enda dokumentatsioon soovitab klientidel lubada. Näiteks suurpank HSBC suutis küll blokeerida välise track.js faili laadimise ja andmete varguse, kuid 'unsafe-eval' lubas ründaja koodi varukoopial panga lehel ikkagi käivituda.

Mida peaksid tegema veebikülastajad ja lehehaldurid?

Kui külastasid esmaspäeval, 16. novembril mõnda nimekirjas olnud veebilehte või kasutad oma ettevõttes Optimizely platvormi, tasub üle kontrollida järgmised turvasammud:

- Uuenda oma Apple'i seadmeid: Paigalda iPhone'ile ja iPadile kohe iOS 18.7.3 (või uuem) või iOS 26.3 (või uuem). Kui kasutasid esmaspäeval mõnel nakatunud lehel vanemat versiooni (iOS 18.6 või varasem), lase seadet võimaliku kompromiteerimise suhtes kontrollida.

- Kontrolli krüptoülekandeid ja pangakaarte: Kui tegid esmaspäeval krüptomakseid, võrdle saaja aadressi sellega, kuhu plaanisid raha saata, ning kontrolli aadresse alati riistvaralise rahakoti füüsiliselt ekraanilt. Kui sisestasid mõnel mõjutatud lehel pangakaardi andmeid otse lehe vormi, jälgi hoolikalt konto väljavõtet või vaheta kaart välja.

- Puhasta ja auditeeri Optimizely projektid (veebihalduritele): Vaata üle kõikide projektide Project JavaScript ja eksperimentide lisakood ning otsi sealt viiteid stringidele 1688360, .icu, track.js või atob(. Vaheta välja kõik API-võtmed, paroolid ja ilma HttpOnly liputa küpsistes hoitud sessioonivõtmed ning seadista range CSP, mis piirab connect-src ühendusi ja väldib 'unsafe-eval' kasutamist.

- Uudised

- Tarkvara
- Turvalisus

Pilt

