Az „AdFection” tanulságai és most mit tegyünk

PCLinuxOS Magazine - 2026. november

Írta: Bill Budington és Thorin Klosowski
Electronic Frontier Foundation
Újranyomva Creative Commons licence alapján



A múlt héten a Citizen Lab kutatói egy új, szörnyű rosszindulatú támadássorozatot fedeztek fel, amit „AdFection”-nek neveztek el. Hirdetési hálózatot használva fertőztek meg kémprogrammal újságírók eszközeit anélkül, hogy a célpontnak bármire is kattintania kellett volna. Ez a fajta újságírók elleni támadás veszélyes és hihetetlenül aggasztó, különösen azért, mert egy olyan technológiára épül, amit miatt már szót emeltünk: a behavioral advertising (viselkedésfüggő hirdetés). Bár e fajta támadás csak újságírókkal kapcsolatban merült fel, a következő szakaszban felvázolunk néhány lépést, hogy csökkentsük a kockázatot, érintettségtől függetlenül.

Pár tényező együttesen teszi ezt a támadást figyelemre méltó első ilyen jellegűvé. Először is, a megfigyeléses hirdetési technológiát használta a rosszindulatú kód célzására. Másodszor, az általa szállított kémprogram úgynevezett „nulla kattintású”, ami azt jelenti, hogy a fertőzéshez nem kell felhasználói inter-akció: mindössze kézbesíteni kellett a hirdetést, és a vele együtt csomagolt kódot a futtatáshoz, ami automatikusan megtörténik. Sem a rosszindulatú támadások, sem a zéró kattintásos támadások önmagukban nem újak. Az AdFection támadásban az új az, hogy kombinálják ezeket, létrehozva egy különlegesen célzott, rendkívül veszélyes támadást, ami ellen nehéz védekezni, és még nehezebb észlelni.

Vizsgáljuk meg alaposabban az Al Jazeera-tól kutatóknak átadott Windows-eszközök egyikének oldaláról. A jelentés így írja le a fertőzést:

Valaki az adott gépen böngészi az Internetet, vagy egy futtatott alkalmazása kap egy hirdetést a Discover-Tech-től, ami a jelentésben „jogosult reklámcégnek mutatja magát, [de] úgy tűnik, hogy nagyszabású kémkedést takar.”

* A hirdetés tartalmaz egy rövid JavaScript-kódrészletet, ami automatikusan lefut, amikor megjelenik az alkalmazásban vagy a weblapon.

* A kód visszajelez egy Discover-Tech szervernek, amire „NOAS-kiszolgálójaként” hivatkozik, és részletes információkat ad a



géptől, ami megjeleníti: a cookie-készlet hirdetési azonosítóját, IP-címét és még sok mást.

Eddig semmi szokatlan nincs ebben. A JavaScript-kódot tartalmazó hirdetések, és a szervereikhez való visszajelzése információkkal az eszközről – és áttételesen Önről – mindennapos. Mindez az adatvezérelt hirdetési ökoszisztéma része. Ami ezután történik, az sokkal érdekesebb:

* A NOAS szerver ezeket a részletes információkat használja annak megállapítására, hogy egy Al Jazeera gép kéri a hirdetést.

* Ahelyett, hogy üres választ adna vissza (ahogy az többnyire történik), rosszindulatú, nulla kattintásos kémprogram „hasznos teherrel” válaszol. Ezt a hasznos terhet a Discover-Tech partnere, a Candiru/Integrity Labs készítette, amit korábban fejlett rosszindulatú programtámadásokban való részvevőként azonosítottak.

* A „hasznos teher” ezután lefut, és megfertőzi a megcélzott gépet.

Ahogy cégek zéró kattintásos rosszindulatú programmal céloznak meg az újságírókat, akár kasszasiker kémthriller cselekménye is lehetne. A támadást azonban a felhasználók adatainak gyűjtésében sajnálatosan széles mozgástérrel rendelkező ad-tech cégek napi gyakorlata tette lehetővé. Az eszközökön gyűjtött nyomkövető azonosítók és a célzott hirdetések eljuttatása céljából gyűjtött adatok alkalmasak személyek azonosítására, és a hivatásos kémprogram-vállalkozások újrahasznosíthatják ezeket annak érdekében, hogy finomhangolják, kit fertőznek meg – és hogy elrejtsék ténykedésüket mindenki más elől.

A legtöbb hirdetést nem közvetlenül a hirdetést készítői, hanem a valós idejű ajánlattételi aukciós közvetítők küldik. Ennek ellenére a nyertes ajánlattevők lehetőséget kapnak arra, hogy JavaScript-kódot hajtsanak végre a megcélzott hirdetést fogadó személy böngészőjében. Ez lehetővé teszi interaktív hirdetések megjelenítését, de (ahogy láttuk) az eszköz kompromittálását is, rosszindulatú kód kézbesítésével.

Bár a támadási lánc összetevői önmagukban nem újak, ennek a kombinált támadásnak a felfedezése fontos, mert feltárja a kiemelten célzott egyének és szervezetek megfertőzésének technikáját. Szerencsére vannak olyan lépések, amikkel megvédheti magát a reklámipar miatti számtalan veszélytől. Íme, hogy lehet:

Amit ellene tehetsz

Miközben a hirdetési ökoszisztéma alapvető javításán és a behavioral adv. teljes betiltása érdekében dolgozunk, mindenkinek feladata, hogy megvédje magát. Ez különösen fontos a fokozott kockázatú személyek vagy újságírók számára, akik erősen kontrollált államokban dolgoznak. A Citizen Lab több lépést is felvázolt, amiket a fenyegetettségtől függően, meg kell tenni az önvédelem érdekében:

Azonnal zárolja az eszközt pár egyszerű lépéssel.

Építs ki erős biztonsági alapot. Az olyan webhelyek, mint a mi Surveillance Self-Defense-ünk és a Consumer Reports biztonsági tervezője (Security Planner) segíthetnek az indulásban.

Használj böngészőbővítményt a nyomon követés csökkentésére. A Privacy Badger bővítmény kiváló kezdet lehet. Hálózati szintű hirdetésblokkoló szolgáltatást is érdemes fontolóra venni, ha járatos vagy a beállítási folyamatban.

Mobiltelefonon tiltsd le vagy töröld az AD ID-t (hirdetésazonosító). Itt vannak a lépések Android és iPhone telefonra.

Fontold meg erősebb adatvédelemmel rendelkező böngésző használatát.

Ezek a lépések nagyon hasznosak lehetnek az önvédelemre, de magánemberként csak ennyit tehetsz. A Behavioral ads betiltása jó kiindulópont lenne. A Behavioral ads kialakítása nem csak adatvédelmi rémálom. Tökéletes eszköz a rosszindulatú és hasonló fenyegetésekhez, ahogy itt láthattuk.

Looking for an old article?
Can't find what you want?

Try the PCLinuxOS Magazine's searchable index!

The PCLinuxOS magazine