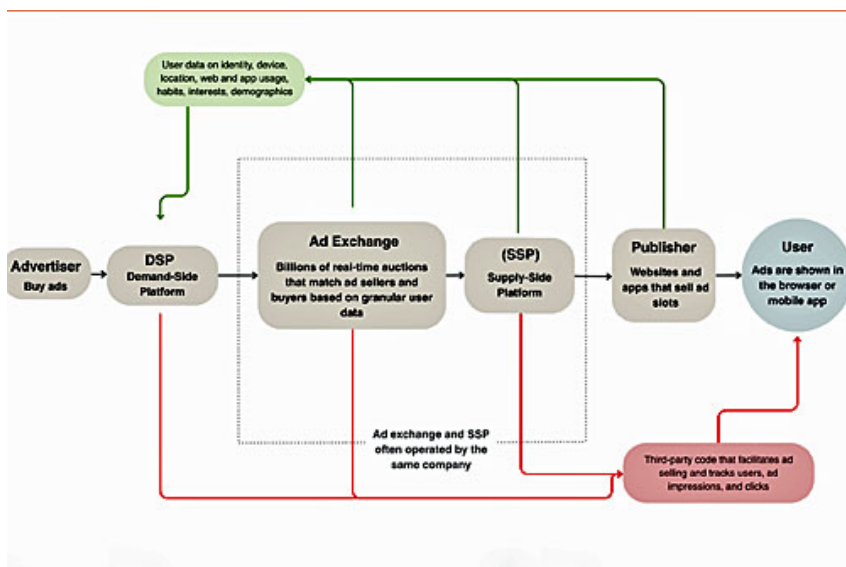


Reklamy internetowe do ataków szpiegowskich

#Cyberprzestrzeń #Nowe technologie #Strategia i polityka 17 października 2026

Izraelska Discover-Tech z Tel Awiwu wykorzystywała globalną sieć reklam internetowych do gromadzenia danych osobowych i przeprowadzania ataków szpiegowskich na wybrane urządzenia. Działając oficjalnie w branży reklamy cyfrowej, wykorzystywała infrastrukturę popularnych platform, w tym Google, Yandex i Beeswax, do identyfikowania użytkowników Internetu oraz dostarczania oprogramowania szpiegowskiego na ściśle wybrane urządzenia. Ustalenia te przedstawili 15 października 2026 badacze kanadyjskiego Citizen Lab i amerykańskiego Confiat zajmującego się cyberbezpieczeństwem.

Badacze nazwali tę metodę AdFection. Umożliwia ona przeprowadzanie ataków typu zero-click, czyli bez konieczności klikania w reklamę, otwierania podejrzanych linków czy pobierania plików. Wystarczy wyświetlenie odpowiednio przygotowanej reklamy na urządzeniu wybranej osoby. Po zainfekowaniu urządzenie zostaje przekierowane do infrastruktury wykorzystywanej do dostarczenia złośliwego oprogramowania. Umożliwia ono przejmowanie poufnych informacji, w tym wiadomości, dokumentów i danych logowania, a także uzyskiwanie dostępu do wybranych funkcji urządzenia. Według Citizen Lab, wykorzystanie tej metody przez Discover-Tech jest pierwszym publicznie udokumentowanym technicznie przypadkiem wykorzystania metody AdFection.



Podstawowa architektura ekosystemu reklamy internetowej / Ilustracja: Citizen Lab

Izraelskie przedsiębiorstwo systemem o nazwie Controlium atakowało przede wszystkim obszar Palestyny (do 10% aktywności), a wśród celów operacji znaleźli się pracownicy telewizji Al Jazeera. Szczególnie

intensywną aktywność odnotowano na urządzeniach z systemem Android, gdzie średnio jedna na 36 reklam pochodziła z infrastruktury Discover-Tech.

Oprogramowanie opracowała izraelska Candiru, także z Tel Awiwu. W 2021 została ona umieszczona na amerykańskiej czarnej liście przedsiębiorstw ze względu na działalność związaną z cyberinwigilacją. Obecnie działa pod nazwą Integrity Labs (w

2025 aktywa i pracownicy Candiru zostali przejęci przez amerykańską Integrity Partners za 30 mln USD, by ominąć sankcje). To na serwery Candiru były przekierowywane urządzenia zainfekowane przez reklamy dostarczane przez Discover-Tech.

Confiant przeanalizował około 4 miliardów rekordów związanych z aukcjami reklam. Ustalono, że w ciągu 4 miesięcy reklamy Discover-Tech pojawiły się na niemal 200 tys. różnych stron internetowych i aplikacji mobilnych działających na Androidzie i iOS. Według badaczy infrastruktura przedsiębiorstwa obsługiwała około 10 milionów wyświetleń reklam dziennie.

Aktywność Discover-Tech odnotowano m.in. w sieciach wykorzystywanych przez instytucje państwowe, organizacje międzynarodowe, sądy, uniwersytety i podmioty związane z obronnością. Wśród nich znalazła się infrastruktura biura premiera Armenii. Badacze wykryli kierowanie wybranych urządzeń do serwerów Candiru w 9 państwach. Największy udział, wynoszący 56% zaobserwowanej aktywności tego rodzaju, przypadł Belgii. Kolejne przypadki odnotowano między innymi w Arabii Saudyjskiej, Bahrajnie, Hiszpanii, Meksyku i Zjednoczonych Emiratach Arabskich. Eksperti zastrzegają, że sama obecność reklam Discover-Tech w sieciach instytucjonalnych nie oznacza, iż doszło do skutecznego włamania. Potwierdza natomiast zasięg infrastruktury, którą można było wykorzystywać do rozpoznawania potencjalnych celów.

Po ujawnieniu wyników dochodzenia największe podmioty branży reklamowej rozpoczęły blokowanie dostępu Discover-Tech do swoich platform. Google zakończyło współpracę z izraelskim przedsiębiorstwem i uniemożliwiło mu korzystanie z własnej infrastruktury reklamowej. Podobne działania podjęły Beeswax, Vungle i Eskimi, a europejska organizacja branżowa IAB Europe wykluczyła przedsiębiorstwo ze swojego systemu.