next.ink

Une régie publicitaire surveillait plus de 5 milliards de portables via 500 000 applications - Next

Jean-Marc Manach

8–11 minutes

Patternz avait été conçue pour le « *suivi, traçage et surveillance* » des téléphones portables à des fins de sécurité nationale. Son directeur technique avait par ailleurs élaboré l'architecture de la première version du logiciel espion Pegasus.

Des centaines de milliers d'applications faisaient partie d'un « *puissant outil de surveillance de masse* », Patternz, susceptible de surveiller l'emplacement physique, les loisirs et les membres de la famille de leurs utilisateurs, révèle 404 Media.

Son enquête s'appuie sur des documents marketing et des vidéos désormais supprimés, une analyse technique légale et des recherches menées par des défenseurs de la protection de la vie privée. Elle a conduit Google et PubMatic, une autre société de publicité, à couper les ponts avec la régie publicitaire liée à ce prestataire de surveillance.

Dans une vidéo téléchargée sur YouTube en janvier 2023, qui a été retirée après que 404 Media lui ait posé des questions, Rafi Ton, qui se présentait comme le PDG de Patternz, déclarait « *nous analysons le comportement de plus de 600 000*

applications ».

Une diapositive indiquait que « *le téléphone portable devient de facto un bracelet de tracking* » et suggérait que le suivi pouvait être réalisé par « *pratiquement n'importe quelle application relayant des publicités* ».

Ton reconnaissait que Patternz avait été conçue comme une « *plateforme de sécurité intérieure* ». D'autres documents de marketing en ligne indiquaient qu'elle s'adresse spécifiquement aux « *agences de sécurité nationale* » pour les aider à « *détecter les modèles d'audience et le comportement des utilisateurs grâce à l'exploration et à l'analyse de données sur la publicité numérique* ».

Plus de 90 To de données par jour, plus de 5 milliards d'identifiants

Dans la vidéo, Ton cliquait sur un profil particulier, révélant une longue liste de coordonnées GPS, les adresses correspondantes, les lieux fréquemment visités, les applications utilisées, la marque du téléphone et son système d'exploitation,

ainsi qu'une liste des autres utilisateurs qui se trouvaient à côté de la cible lorsqu'ils étaient à la maison et au travail.

L'Irish Council for Civil Liberties (ICCL), l'ONG irlandaise qui avait révélé son existence en novembre 2023, soulignait en outre que l'entreprise israélienne (qui vantait les mérites de Patternz) expliquait que la plateforme, conçue pour le « *suivi, traçage et surveillance* » des téléphones portables à des fins de sécurité nationale, pouvait également identifier les enfants, membres de la famille et collègues des personnes ciblées.

Les utilisateurs de Patternz pouvaient créer des alertes pour ce qu'ils considèrent comme des événements importants, tels que « *l'arrivée d'une personne à un endroit, le départ d'une personne d'un endroit, la rencontre d'une personne avec une autre personne* », ajoutait Ton dans la vidéo.

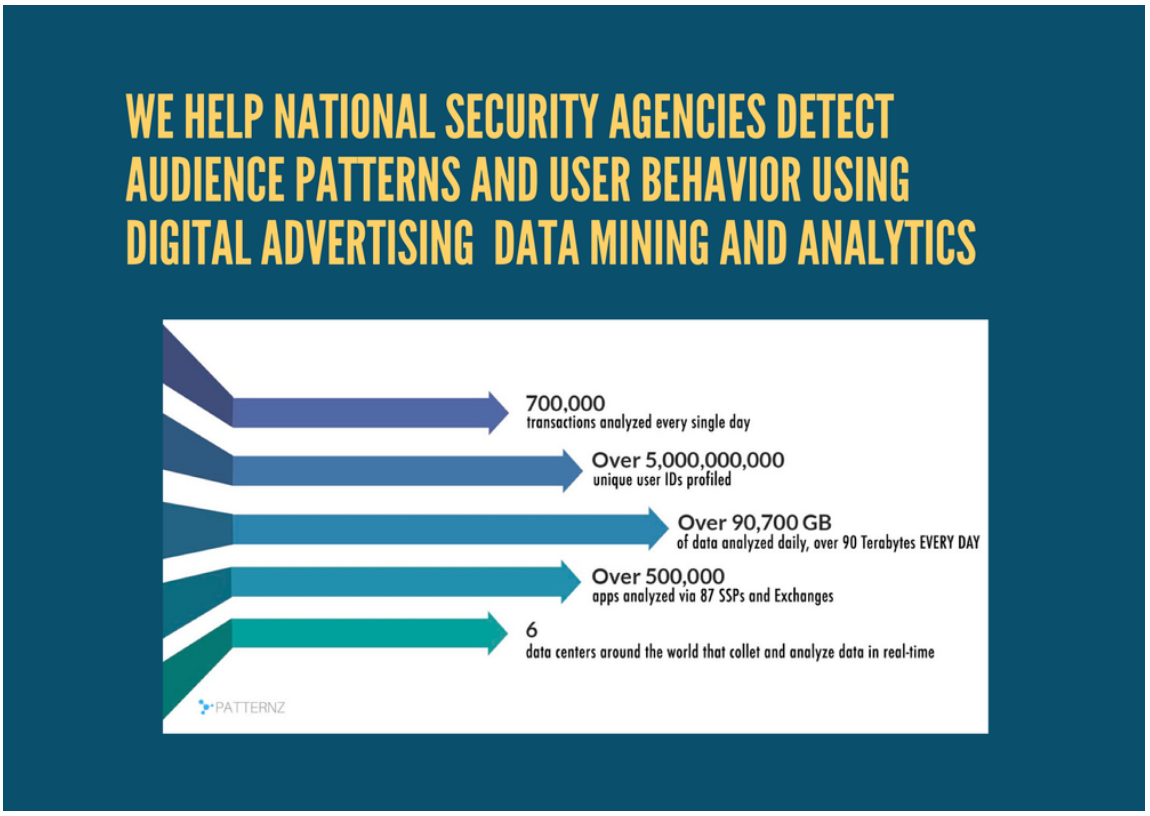
Des documents de marketing indiquent que la plateforme analyse « *plus de 90 téraoctets de données par jour* », et disposer des profils de « *plus de 5 milliards d'identifiants d'utilisateurs* ». « *Chaque appareil possède un identifiant unique, à partir duquel nous pouvons créer un profil* », expliquait

M. Ton.

La face cachée d'une régie de publicités ciblées

Sur Twitter, Wolfie Christie, co-auteur du rapport de l'ICCL, relevait que Patternz expliquait que son système était « *construit sur le savoir-faire étendu de l'exploitation d'une plateforme d'enchères en temps réel au cours des cinq dernières années* ».

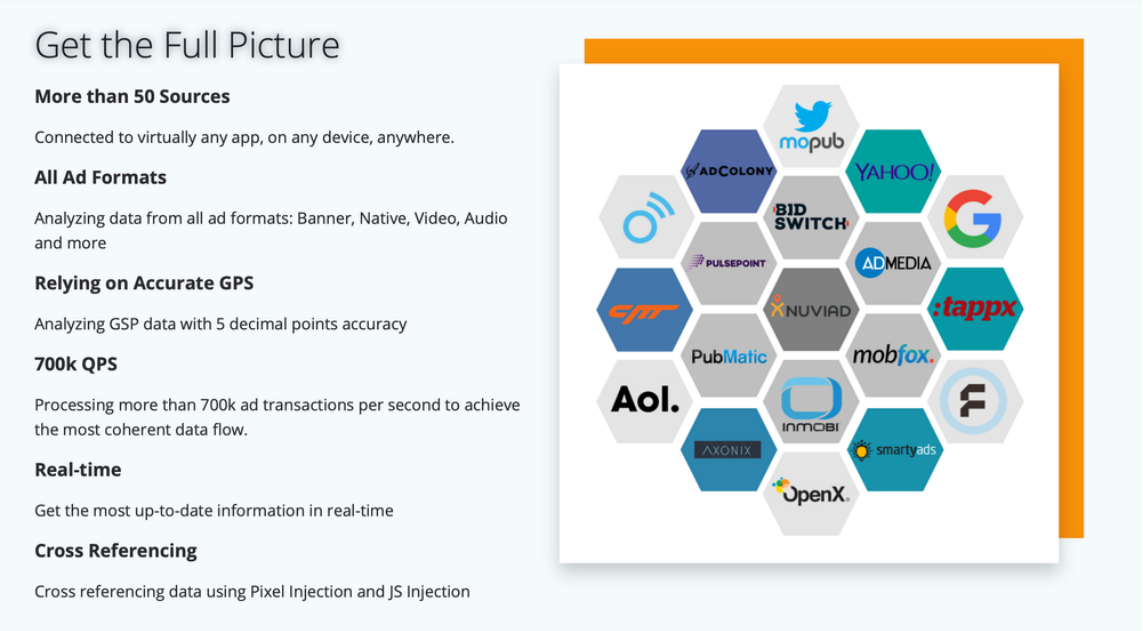
Un autre document marketing publié sur le site web d'une organisation de sécurité israélienne indique même que Patternz peut aussi être utilisé pour déployer des logiciels malveillants, « *envoyer des messages ciblés, des publicités ou des chevaux de Troie directement via la pile AdTech pour des résultats optimaux* ».



La version de démonstration de Patternz montrée dans la vidéo prétend disposer de données provenant de 177 431 applications Android et 61 894 applications iOS. Mais un document marketing évalue le nombre total d'applications connectées à

Patternz à plus de 500 000, analysées en temps réel via 87 partenaires, à travers six datacenters partout dans le monde.

Dans l'un des documents marketing désormais supprimés, Patternz indiquait disposer d'une « *branche AdTech entièrement commerciale et opérationnelle* ». Y figurait une infographie désignant 19 entreprises, dont Google, Yahoo, MoPub (l'ancien réseau publicitaire de Twitter), PubMatic, BidSwitch, InMobi, etc. avec, au centre de l'infographie, Nuviad.



Or, Rafi Ton est aussi le PDG de Nuviad, une entreprise spécialisée dans le Real Time Bidding (RTB), une technologie consistant à vendre ou acheter en temps réel et au plus offrant de la publicité ciblée.

Son ancien site proposait ainsi de « *cibler la bonne personne, au meilleur moment et à l'endroit idéal* » en utilisant l'identifiant des appareils et « *le reciblage basé sur IP pour des campagnes publicitaires plus personnalisées* ».

Le directeur technique qui avait élaboré l'architecture de Pegasus

Intelligence Online révèle par ailleurs que le directeur technique

de Patternz, Yigal Unna, avait préalablement été celui de NSO qui, de 2010 à 2014, d'après le New York Times, avait « *inventé l'architecture Pegasus et dirigé l'équipe qui a écrit le code derrière la première version du logiciel espion* ».

- 

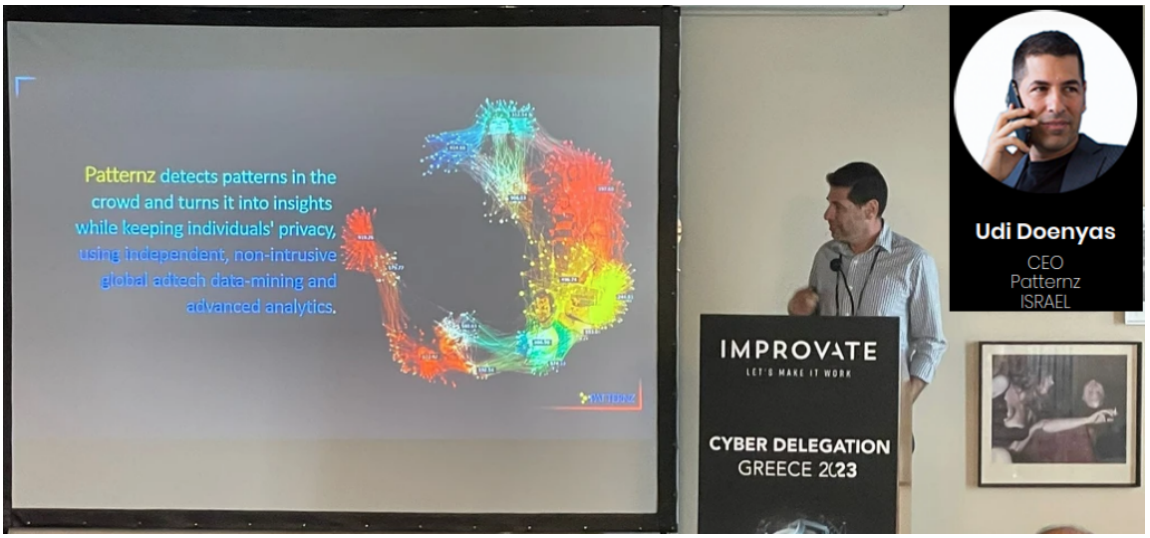
Pegasus : 50 000 « cibles potentielles » ? (1/2)

- 

Pegasus : 50 000 « cibles potentielles » ? (2/2)

En septembre 2023, Yigal Unna était en effet présenté comme le CEO de Patternz dans un voyage d'affaires dirigé par Yigal Unna – ancien directeur général de la Direction nationale

israélienne de la cybersécurité censée présenter les « *meilleures innovations et technologies de cybersécurité* » israéliennes à des responsables gouvernementaux des agences de renseignement et forces de l'ordre grecs.



Improvate.net

Or, le cabinet israélien de développement commercial Improvate The Future (ITF), qui organisait la délégation, a assigné Patternz, le 18 janvier, devant les tribunaux de Tel-Aviv pour des prestations impayées.

Non content de laisser traîner sur le web, et sans les protéger, des plaquettes marketing et vidéos révélant l'ampleur de ce à quoi sa plateforme pouvait servir, Patternz n'a donc pas non plus chercher à cacher que son infrastructure aurait été, sinon conçue, en tout cas supervisée par l'architecte technique du logiciel espion Pegasus.

« Bravo !!! Vous venez de tuer une entreprise. »

Plusieurs autres médias, rappelle 404 Media, avaient déjà enquêté sur l'utilisation de ces enchères publicitaires en temps réel par des forces de l'ordre et services de renseignement, une technique surnommée ADINT (pour ADvertising INTelligence).

En mai, Bloomberg avait ainsi publié une enquête centrée sur une société de surveillance israélienne appelée Rayzone Group, qui a acquis des sociétés de technologie publicitaire et s'est également fait passer pour des annonceurs potentiels afin de récolter des données.

En septembre, Hareetz avait publié sa propre enquête sur d'autres sociétés israéliennes ayant, elles aussi, développé cette capacité. Le Wall Street Journal avait, lui aussi, enquêté, en octobre, sur ces entreprises publicitaires permettant aux autorités d'acheter des données « en masse », collectées à partir de publicités, pour faciliter la surveillance gouvernementale.

« *Nous prenons au sérieux notre responsabilité de protéger la vie privée des gens, c'est pourquoi nous avons les restrictions les plus strictes du secteur sur les types de données que nous partageons dans le cadre des enchères en temps réel. Nous ne partageons pas de localisation précise ni de données personnelles sensibles avec les acheteurs RTB et nos politiques interdisent tout effort visant à identifier ou à créer des profils d'individus sur la base de données sensibles* », a déclaré un porte-parole de Google à 404 Media dans un communiqué.

Le sénateur démocrate états-unien Ron Wyden explique à 404 Media avoir alerté Google dès 2021, et l'avoir relancé à plusieurs reprises depuis, dont trois fois rien qu'en ce mois de janvier. S'il se félicite que Google a enfin accepté d'empêcher Nuviad d'accéder aux données de ses utilisateurs, il regrette de voir qu'il a fallu attendre qu'un journaliste ne leur pose des questions, faisant planer la menace d'une mauvaise publicité, pour que Google protège enfin ses utilisateurs.

Lorsqu'on lui a demandé de commenter l'exclusion de son

entreprise par Google, un responsable de Nuviad a répondu à 404 Media : « *Bravo !!! Vous venez de tuer une entreprise. L'impact est simple : Nuviad est morte* ».